

## LA-UR-21-27042

Approved for public release; distribution is unlimited.

Title: Classified Matter Protection and Control User Refresher Training  
Course 35043

Author(s): Rinke, Helen Mae

Intended for: Web

Issued: 2021-07-20

---

**Disclaimer:**

Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by Triad National Security, LLC for the National Nuclear Security Administration of U.S. Department of Energy under contract 89233218CNA000001. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

# Classified Matter Protection and Control

## User Refresher Training

### Course 35043

## Introduction

Welcome to the Classified Matter Protection and Control Refresher Training for users of classified matter. The purpose of this refresher training is to familiarize workers with responsibilities of protecting and controlling classified matter. This biannual training must be completed by all workers whose job duties include generating, processing, accessing, handling, using, storing, reproducing, destroying, transmitting or accounting for classified matter.

*Classified Matter Protection and Control User Refresher Training Course #35043 has been Designated Unclassified Subject Areas (DUSA) - Designator: TRNG.*

## Notice of Violation

A violation of the provisions of the Classified Matter Protection and Control Handbook relating to the safeguarding or security of Restricted Data (RD) or other classified information may result in a civil penalty to subsection a. of section 234B of the Atomic Energy Act of 1954 (42 U.S.C. 2282b). The procedures for the assessment of civil penalties are set forth in 10 CFR 824, Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations.

Working with classified matter is serious business. For the sake of national security we must all be reminded of the responsibilities we have been entrusted with. Workers are encouraged to ask questions and seek guidance before working with classified matter.

## Using This Course

This course features some dynamic components as well as a number of optional keyboard commands.

Pressing the **M** key will toggle display of the Table of Contents for this course, as will clicking on the **Contents** handle at left.

Use the **buttons** that appear at the bottom-right to move forwards and backwards through this course. You can also use the **Left** and **Right Cursor Keys** to navigate.

You can adjust the **font size** using the controls on the lower left side of the page. You can also use the **1** through **5** keys on your keyboard, where **1** is **extra small** and **5** is **extra large**. Your font size preference will be remembered for up to a year, less if you delete your web browser's cookies.

To be sure you see all the content, scroll to the bottom of each page.

## Course Objectives

1. Identify classified matter
2. Identify methods of generating classified matter
3. Identify protection and control requirements
4. Identify storage requirements
5. Identify requirements for marking documents, working papers, E-mail, CREM, parts
6. Identify reproduction requirements
7. Identify requirements for transmission mail, hand-carry, fax, E-mail
8. Identify destruction requirements
9. Identify requirements for accountability, emergency situations and reporting incidents of security concern
10. Be aware of points of contact and reference documents for working with classified matter

Upon completion of this course, you will be familiar with your responsibilities for accessing, handling and owning classified matter. In this course we will define classified matter and discuss the generation, protection, control and storage of classified matter. We will also review how to mark, reproduce, transmit and destroy classified matter. We will look into accountability requirements for certain types of classified matter. Additionally, we will examine how to handle classified matter during emergency situations as well as how to report incidents of security concern. Lastly, you will become familiar with points of contact and reference documents for working with classified matter.

## Objective 1: Identifying Classified Matter

- Marking terms: level, category and caveats
- Types of classified matter

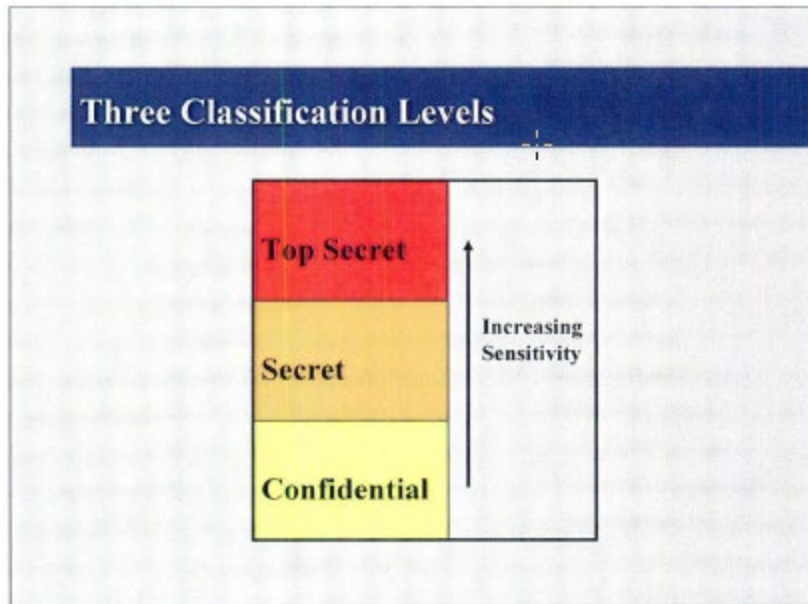
Objective I: Identify classified matter. What is classified matter? In this section we will define marking terms such as level, category and caveats and identify the different types of classified matter.

## Identifying Classified Matter

| Classification Level & Category |                 |                          |                               |                             |
|---------------------------------|-----------------|--------------------------|-------------------------------|-----------------------------|
|                                 | Restricted Data | Formerly Restricted Data | National Security Information | Increasing Sensitivity<br>↑ |
| Top Secret                      | TSRD            | TSFRD                    | TSNSI                         |                             |
| Secret                          | SRD             | SFRD                     | SNSI                          |                             |
| Confidential                    | CRD             | CFRD                     | CNSI                          |                             |
| ← Increasing Restrictiveness    |                 |                          |                               |                             |

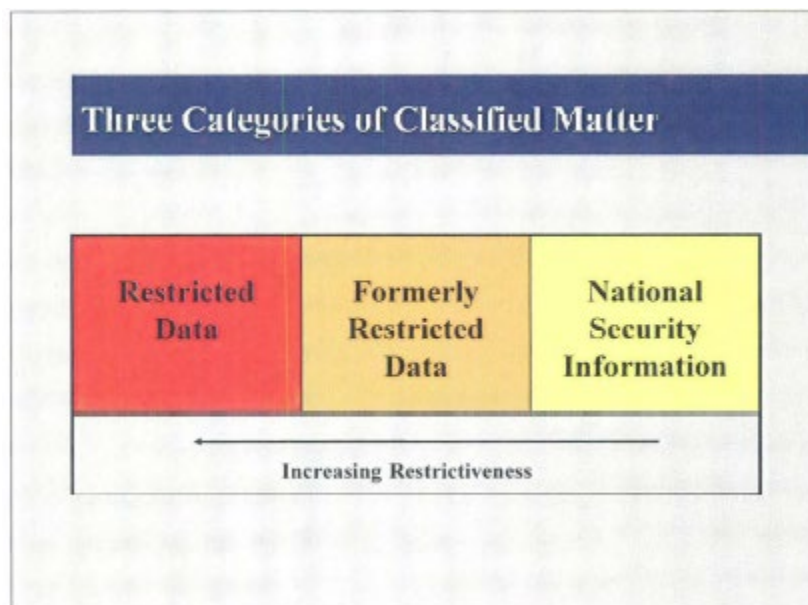
In order for a document, part, or piece of media to be classified, it must be assigned a classification level and category.

---



The classification level is a designation assigned to specific elements of information based on the potential damage to national security if disclosed to unauthorized people. The three classification levels in descending order of potential damage are top secret, secret, and confidential.

---



Classification categories describe the type of information. The three categories of classified information are: restricted data, formerly restricted data and nation security information.

## Classification Level and Category

| Classification Level & Category |                 |                          |                               |                             |
|---------------------------------|-----------------|--------------------------|-------------------------------|-----------------------------|
|                                 | Restricted Data | Formerly Restricted Data | National Security Information | Increasing Sensitivity<br>↑ |
| Top Secret                      | TSRD            | TSFRD                    | TSNSI                         |                             |
| Secret                          | SRD             | SFRD                     | SNSI                          |                             |
| Confidential                    | CRD             | CFRD                     | CNSI                          |                             |
| ← Increasing Restrictiveness    |                 |                          |                               |                             |

Ultimately, restrictions and requirements placed on classified matter are determined by combining classification level and category.

---

## Caveats

| Caveats              |  |
|----------------------|--|
| Abbreviation/Marking | Caveat   |
| NOFORN               | No Foreign Dissemination   |
| REL TO               | Authorized for Release to (name of country or countries)   |
| RELIDO               | Releasable by Information Disclosure Official  |
| ORCON                | Originator Controlled  |
| PROPIN               | Proprietary Information  |
| NATO                 | North Atlantic Treaty Organization   |
| FGI                  | Foreign Government Information   |
| SIGMA or Σ           | Sigma (a number or series of numbers will follow to list the category of Sigma information; i.e., 14, 15, 18, or 20) |
| CNWDI                | Critical Nuclear Weapons Design Information  |
| NNPI                 | Naval Nuclear Propulsion Information   |

Caveat markings are placed on classified matter either to identify special handling and dissemination requirements or to describe the type of information and who originated the information. Here is a list of common caveats.



# Requirements for Viewing Classified Matter

| Three Main Requirements for Viewing Classified Matter |                 |                          |                               |
|---|-----------------|--------------------------|-------------------------------|
|   | Restricted Data | Formerly Restricted Data | National Security Information |
| Top Secret  | TSRD<br>Q       | TSFRD<br>Q               | TSNSI<br>Q                    |
| Secret  | SRD<br>Q        | SFRD<br>Q/L              | SNSI<br>Q/L                   |
| Confidential  | CRD<br>Q/L      | CFRD<br>Q/L              | CNSI<br>Q/L                   |

- Proper clearance level
- Need-to-know
- Proper Sigma authorities (Q-clearance require)

There are three main requirements for viewing classified matter. First, individuals must have the proper clearance level. To view any classified matter that contains Top Secret information or Secret Restricted Data, a Q clearance is required. For any other level and category, a Q or L clearance is required. Second, individuals must have a need-to-know the information. According to the Department of Energy, an individual who has a need-to-know needs the classified information in order to complete a job or task that they have been assigned. Third, Q-cleared individuals must be assigned proper Sigma authorities before working with classified matter that contains Sigma levels. Sigmas are considered caveats relating to Restricted Data and/or Formerly Restricted Data concerning the theory, design, manufacture, storage, characteristics, performance, effects or use of nuclear weapons, nuclear weapon components, or nuclear explosive devices or materials.

## Types of Classified Matter

## Types of Classified Matter

Classified matter includes:

- Documents (E-mails, working papers/drafts, facsimiles, graphs and charts)
- Motion picture film or videotape
- Magnetic, electronic or sound recordings
- Microfiche or microfilm
- Photographic prints
- Transparencies, slides or sheet film
- Radiographs, X-rays or aperture cards
- ~~Parts~~
- Electronic media (Hard drives, CDs, Zips, floppies, thumb drives, flash cards, etc.)

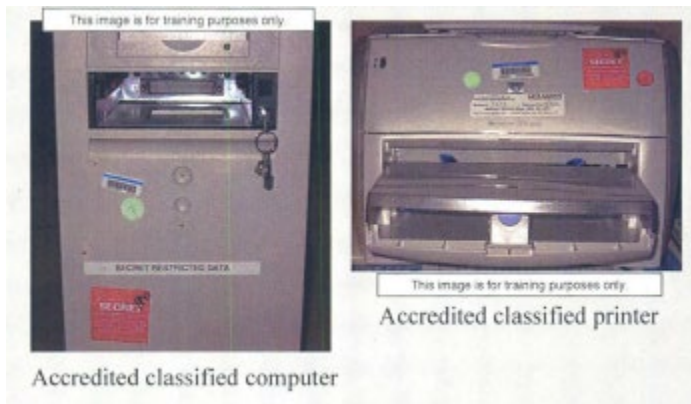
If you have a clearance, you must understand that you are trusted with our national security. That security rests in your hands when you work with classified matter. Classified matter can be found in many different physical forms. Here are a few examples of what could be considered classified matter: documents; film or videotapes; magnetic, electronic or sound recordings; microfiche or microfilm; photographic prints; transparencies, slides or sheet film; radiographs, X-rays or aperture cards; parts or electronic media

## Objective 2: Identify Methods of Generating Classified Matter

Identify methods of generating classified matter. In this section we will identify the:

- Methods used to generate classified matter
- How Classified Removable Electronic Media also known as (CREM) is created

## Methods of Generating Classified Matter



The most common method of creating classified matter is by simply using a computer accredited for processing classified information. Entering classified information into the classified computer and then printing it out creates a classified document, drawing, design or graphic. Saving the same information onto a zip drive creates a piece of classified removable electronic media or CREM.

---

## Other Methods of Generating Classified Matter

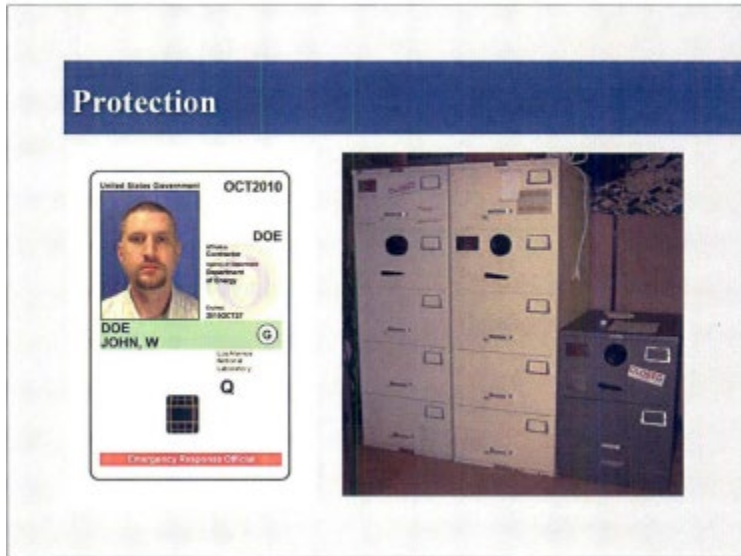
- Classified E-mail
- Taking photographs of classified items or activities
- Recording classified discussions
- Machining metal into classified shapes
- Handwriting classified notes or documents
- Writing classified comments on unclassified documents

There are many other ways to create classified matter; one is by E-mail. Sending classified E-mail is allowed only on the secured, classified network. If you are not using the secured, classified network, you must be careful not to add information to other E-mails that may make the sum total of the E-mails classified. Other ways to generate classified matter cover a diverse and wide-ranging list of activities.

## Objective 3: Identify protection and Control Requirements

- Identify rules regarding protection of all classified matter
- Determine need-to-know
- Identify potential consequences of not protecting classified matter

## Protection



Only properly cleared individuals with a need-to-know and proper authorities are allowed to work with classified matter. Classified discussions and work must be conducted within security areas. Classified matter must always be protected from unauthorized physical, visual or aural access. When classified matter is not in use, it must be stored in a storage container which includes GSA-approved safes, vaults or VTR. Classified matter must not be left unattended at any time.

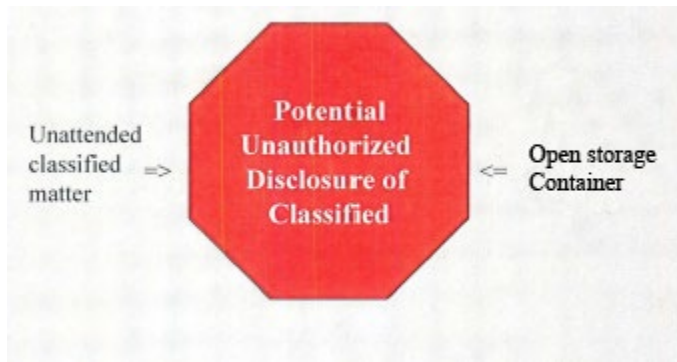
## Need to know



**Curiosity is not the need to know!**

Any worker who has been granted access to classified matter must determine another worker's clearance and need-to-know before granting access to that matter. Need-to-know must be established by determining what matter will be accessed and that the recipient requires access to this matter to perform his or her official duties through current relationships, tasks, duties, and assignments; or confirmation by your Responsible Line Manager. In rare cases, incidental access may be granted to individuals (such as audits by LANL employees or external organizations) who handle or come into contact with classified matter but whose job functions do not include review or other use of the classified matter. If you have questions about granting access to classified matter, contact your RLM. Sigma authorization is also part of need-to-know. Verify the recipient's sigma authorities before passing on classified information that contains Sigma information.

## Consequences

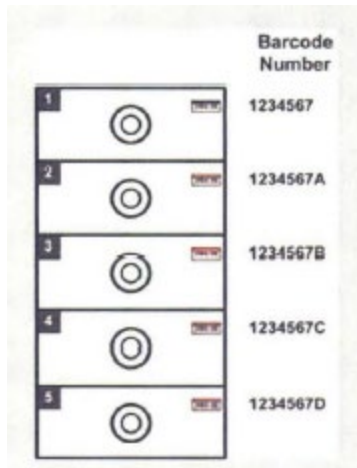


Leaving classified matter unattended or leaving storage containers open may be an incident of security concern. You are responsible for the control of all classified matter under your care. The document's originator is responsible for ensuring that matter created in any subject area that is, or may be, classified is reviewed for classification by a Derivative Classifier and marked appropriately before dissemination.

## Objective 4: Identify Storage Requirements

- Review the procedures for barcodes on GSA-approved storage containers storing classified matter
- Examine the required forms and procedures for completing the forms for storage containers storing classified matter
- Procedures for end-of-day checks of storage containers
- Use of cover sheets

## Barcoding GSA-Approved Storage Containers



- Must be tagged with barcodes
- Must be assigned to a steward
- Trackable via the Sunflower property management database
- Multi-locking storage containers must have a barcode on each locking drawer that stores classified matter

GSA-approved storage containers used to store classified matter must be located in a Limited Area or higher, tagged with a barcode and assigned to a steward. Barcoded storage containers will be tracked via the CMPC safe database, making it easier to locate, manage, and audit storage containers storing classified matter. Multi-locking storage containers (e.g., five-drawer / five-combo) must have a barcode applied to each drawer that stores classified matter. This practice will allow each locking drawer to have a different steward identified in CMPC safe database.

## Steward for Barcoded Safes

- A steward must be assigned for each safe or drawer of a multi-locking safe used to store classified matter
- The steward may be the primary user of a safe storing classified matter
- the safe may not be assigned to a Classified Matter Custodian (CMC), Deployed Security Officer(DSO), or group administrator if they are not owners or users of the classified matter
- A worker co-located with a safe but does not have access to the contents may not be a steward

A LANL worker must be assigned as the steward for each safe or drawer of a multi-locking safe used to store classified matter. Barcoded safes are considered property, to be owned by a steward, much like a computer. The steward may be the primary user of a safe storing classified matter, the RLM, project leader, or another person designated by the RLM. The safe may not be assigned to a CMC, DSO, or group administrator if they are not owners or users of the classified



matter within. A worker who is co-located with a classified safe but does not have access to the contents may not be designated the default steward of the safe.

## Standard Form 700

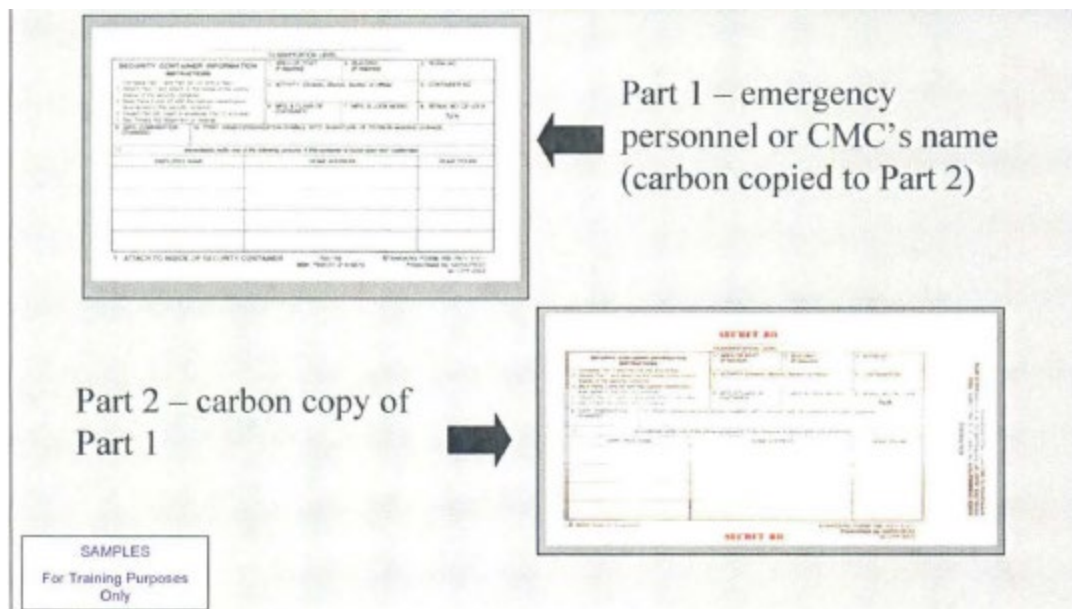
The image displays two versions of Standard Form 700. The top version is a training sample, indicated by a diagonal stamp that reads "SAMPLES For Training Purposes Only". It features a header with classification levels (Secret, Confidential, etc.) and a table for recording information. The bottom version is the actual Standard Form 700, marked with "SECRET RD" in red. It includes a table for recording information and a section for "REMARKS". Both forms have a footer with the text "STANDARD FORM 700 (REV. 4-01) Prescribed by SECRETARY OF DEFENSE".

| CLASSIFICATION LEVEL  | SECRET | CONFIDENTIAL | SECRET | CONFIDENTIAL |
|---|--------|--------------|--------|--------------|
| 1. Complete Part I and Part II of this form and attach to the container in the manner shown on the reverse side of this form. |        |              |        |              |
| 2. Attach this form to the container in the manner shown on the reverse side of this form.                                    |        |              |        |              |
| 3. Attach this form to the container in the manner shown on the reverse side of this form.                                    |        |              |        |              |
| 4. Attach this form to the container in the manner shown on the reverse side of this form.                                    |        |              |        |              |
| 5. Attach this form to the container in the manner shown on the reverse side of this form.                                    |        |              |        |              |
| 6. Attach this form to the container in the manner shown on the reverse side of this form.                                    |        |              |        |              |
| 7. Attach this form to the container in the manner shown on the reverse side of this form.                                    |        |              |        |              |
| 8. Attach this form to the container in the manner shown on the reverse side of this form.                                    |        |              |        |              |
| 9. Attach this form to the container in the manner shown on the reverse side of this form.                                    |        |              |        |              |
| 10. Attach this form to the container in the manner shown on the reverse side of this form.                                   |        |              |        |              |

STANDARD FORM 700 (REV. 4-01)  
Prescribed by SECRETARY OF DEFENSE

Standard Form 700 must be completed for all storage containers including GSA-approved safes, rooms, vaults, VTR, or other approved locations for the storage of classified matter that use a combination lock. Classifier information is not required to be identified on any part of Standard Form 700. Contact your CMC to obtain a Standard Form 700.

## Standard Form 700: Personnel/Custodians



Standard Form 700 is a carbon copy form. As Part I is completed with a pen or typewriter, the information will be copied onto Part 2. The form must be completed with a list of all the workers who know the combination to the storage container. If additional sheets are used to record users, these sheets must be maintained with Part I and Part 2. However, keep in mind, the number of workers with access to the combination to storage containers must be kept to the minimum number to reasonably accommodate the need as determined by the RLM, project leader, etc.

## Standard Form 700: Part 1



| CLASSIFICATION LEVEL  |                              |                              |               |              |            |  |  |  |  |  |  |  |  |  |  |  |  |
|---|------------------------------|------------------------------|---------------|--------------|------------|--|--|--|--|--|--|--|--|--|--|--|--|
| <b>SECURITY CONTAINER INFORMATION INSTRUCTIONS</b><br>1. Complete Part 1 and Part 2A (on end of Part 1).<br>2. Detach Part 1 and attach to the inside of the locking drawer of the security container.<br>3. Mark Parts 2 and 2A with the highest classification level stored in this security container.<br>4. Detach Part 2A, insert in envelope (Part 2) and seal.<br>5. See Privacy Act Statement if an inmate.<br>6. DATE COMBINATION CHANGED<br>7. PRINT NAME/ORGANIZATION SYMBOL WITH SIGNATURE OF PERSON MAKING CHANGE. |                              |                              |               |              |            |  |  |  |  |  |  |  |  |  |  |  |  |
| 1. AREA OR POST<br>(If required)  | 2. BUILDING<br>(If required) | 3. ROOM NO.                  |               |              |            |  |  |  |  |  |  |  |  |  |  |  |  |
| 4. ACTIVITY (Division, Branch, Section or Office)   |                              | 5. CONTAINER NO.             |               |              |            |  |  |  |  |  |  |  |  |  |  |  |  |
| 6. MFG. & CLASS OF CONTAINER  | 7. MFG. & LOCK MODEL         | 8. SERIAL NO. OF LOCK<br>N/A |               |              |            |  |  |  |  |  |  |  |  |  |  |  |  |
| 11. Immediately notify one of the following persons, if this container is found open and unattended:<br><table border="1"> <thead> <tr> <th>EMPLOYEE NAME</th> <th>HOME ADDRESS</th> <th>HOME PHONE</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> </tbody> </table>   |                              |                              | EMPLOYEE NAME | HOME ADDRESS | HOME PHONE |  |  |  |  |  |  |  |  |  |  |  |  |
| EMPLOYEE NAME   | HOME ADDRESS                 | HOME PHONE                   |               |              |            |  |  |  |  |  |  |  |  |  |  |  |  |
|   |                              |                              |               |              |            |  |  |  |  |  |  |  |  |  |  |  |  |
|   |                              |                              |               |              |            |  |  |  |  |  |  |  |  |  |  |  |  |
|   |                              |                              |               |              |            |  |  |  |  |  |  |  |  |  |  |  |  |
|   |                              |                              |               |              |            |  |  |  |  |  |  |  |  |  |  |  |  |
| 1. ATTACH TO INSIDE OF SECURITY CONTAINER<br>700-102<br>NSN 7540-01-214-5372<br>STANDARD FORM 700 (REV. 4-01)<br>Prescribed by NARA/ISOO<br>32 CFR 2003   |                              |                              |               |              |            |  |  |  |  |  |  |  |  |  |  |  |  |

Block #8 may be marked with N/A

SAMPLE  
For Training Purposes Only

Block #8 of the form may be marked with "N/A." Block #8 must not be marked with the serial number of the lock. Workers who will be contacted in an emergency must have their home address and home phone number listed on the Standard Form 700. The complete Part 1 shall then be placed on the inside of the door containing the combination lock on a vault, or VTR, or inside of the locking drawer containing the combination lock on a GSA-approved safe.

## Standard Form 700: Part 2a

**SAMPLE**  
For Training Purposes  
Only

**SECRET RD** Sigma 15

CLASSIFICATION LEVEL

SECURITY CONTAINER NUMBER

COMBINATION

DETACH HERE

Turn to the (Right) (Left) stop at

Turn to the (Right) (Left) stop at

Turn to the (Right) (Left) stop at

Turn to the (Right) (Left) stop at

WARNING

THIS COPY CONTAINS CLASSIFIED INFORMATION WHEN  
COMBINATION IS ENTERED

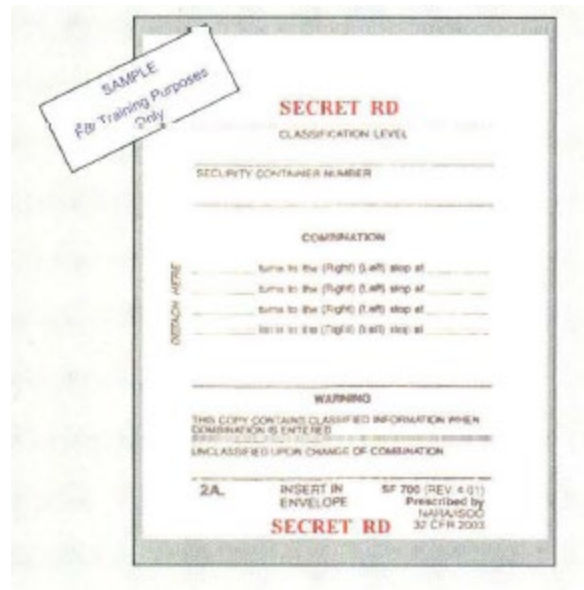
UNCLASSIFIED UPON CHANGE OF COMBINATION

2A. INSERT IN ENVELOPE SF 700 (REV 4-01)  
Prescribed by  
NARA/SOC  
32 CFR 200.3

**SECRET RD**

Part 2a, where the combination is recorded, must be marked top and bottom with the highest level, category and caveats of information contained in the safe, vault or VTR. Part 2a is then placed inside the envelope - Part 2.

## Standard Form 700: Safe Combination



Part 2A is where you record the combination to the safe, vault or VTR.

Combinations to safes, vaults or VTRs must be selected at random. The use of ascending or descending number series or combinations easily associated with the person selecting the combination - such as birth dates or anniversaries - are not permitted.

## Safe Combinations Must Be Changed...

- before initial use of a storage container or lock;
- after maintenance of the storage container by an uncleared technician or locksmith;
- before decommissioning or transferring an empty storage container to another organization, the combination must be set back to factory default setting (50-25-50);
- when a loss, unauthorized disclosure, compromise, or suspected compromise of a storage container or its combination has occurred, to include the discovery that the storage container was left unattended and unsecured;
- when a user no longer requires access due to reassignment, transfer, or termination of employment; or
- when a user's clearance is
  - downgraded to a level lower than the level and category of classified matter stored in the container,
  - suspended, or
  - administratively terminated.

## • Standard Form 702

| STORAGE CONTAINER CHECK SHEET   |            |       |           |      |                    |      |                          |      |  |
|---|------------|-------|-----------|------|--------------------|------|--------------------------|------|--|
| To (if required)  |            |       |           |      | Thru (if required) |      |                          |      |  |
| Certification<br>I certify, by my initials below, that I have opened, closed, or checked this storage container in accordance with pertinent agency regulations and operating instructions. |            |       |           |      |                    |      |                          |      |  |
| Month/Year June 2013  |            |       |           |      |                    |      |                          |      |  |
| Date  | Opened By  |       | Closed By |      | Checked By         |      | Checked By (if required) |      |  |
|   | Initials   | Time  | Initials  | Time | Initials           | Time | Initials                 | Time |  |
| 6/3   | AB         | 8:00  | AB        | 8:30 | YZ                 | 5:00 |                          |      |  |
| 6/4   | BC         | 3:15  | BC        | 4:00 | BC                 | 5:00 |                          |      |  |
| 6/5   | N/A        | _____ |           |      | AB                 | 5:00 |                          |      |  |
| 6/6   | NOT OPENED |       |           |      | YZ                 | 5:00 |                          |      |  |
| 6/7   | _____      |       |           |      | RS                 | 5:00 |                          |      |  |

- **Storage Container Check Sheet**
- Standard Form 702 (also known as LANL Form 1692-A)
- All safe, vault, and VTR activities must be recorded on a Storage Container Check Sheet, which is downloadable from the EIA Online Forms website. The Standard Form 702 is used to record the names or initials of the workers and the times they opened, closed or checked a particular storage container, vault or VTR containing classified matter. The form must be affixed to each container and the entrance to each vault or VTR.

## End of Day Check

| STORAGE CONTAINER CHECK SHEET   |            |       |           |      |                    |      |                          |      |  |
|---|------------|-------|-----------|------|--------------------|------|--------------------------|------|--|
| To (if required)  |            |       |           |      | Thru (if required) |      |                          |      |  |
| Certification<br>I certify, by my initials below, that I have opened, closed, or checked this storage container in accordance with pertinent agency regulations and operating instructions. |            |       |           |      |                    |      |                          |      |  |
| Month/Year June 2013  |            |       |           |      |                    |      |                          |      |  |
| Date  | Opened By  |       | Closed By |      | Checked By         |      | Checked By (if required) |      |  |
|   | Initials   | Time  | Initials  | Time | Initials           | Time | Initials                 | Time |  |
| 6/3   | AB         | 8:00  | AB        | 8:30 | YZ                 | 5:00 |                          |      |  |
| 6/4   | BC         | 3:15  | BC        | 4:00 | BC                 | 5:00 |                          |      |  |
| 6/5   | N/A        | _____ |           |      | AB                 | 5:00 |                          |      |  |
| 6/6   | NOT OPENED |       |           |      | YZ                 | 5:00 |                          |      |  |
| 6/7   | _____      |       |           |      | RS                 | 5:00 |                          |      |  |

Recommendation: Mark "N/A" or similar on Form 702 when the container is not accessed for the day: however, an end-of-day check must still be performed.

An end-of-day check is required every workday for all storage containers, even those that were not accessed that day. The end-of-day check may be performed by a worker other than the user who opened and/or closed the storage container. However, if another worker is not available for an end-of-day check, you may check the container yourself, even if you were the one who opened and closed the container that day. An end-of-day check is not required for storage containers within vaults or VTRs if the vault or VTR was not opened for the day. However, the vault or VTR must be checked. Good business practices suggest marking the storage container check sheet with "NA" for not accessed, not opened or any similar annotation on any particular work day that the storage container was not opened. An end-of-day check must still be performed.

## Cover Sheets - Front and Back



A front cover sheet is a pre-printed page that identifies both the classification level and category of the document. Cover sheets must be applied to all classified documents (including laboratory notebooks) when they are removed from a storage container. Caveats may be written or stamped on the front cover sheet to identify any special handling or dissemination requirements of the



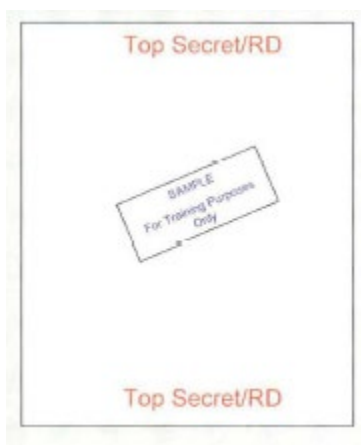
document. The word "accountable" may be written or printed on the front cover sheet for all accountable documents.

When a classified document is removed from a storage container, the back page must also have the classification level on the top and bottom of the page. There are three acceptable ways to meet the requirement for the back page: (1) use a pre-printed routing slip, back cover sheet or cover sheet, (2) use a blank sheet of paper marked with the classification level, or (3) mark the last page of the document with the classification level as long as no text appears on the back of the last page. It is recommended to also mark the category of the document on the back cover sheet or routing sheet.

## Objective 5: Identify Marking Requirements

- Marking requirements for classified documents
- Conditions under which classified draft or working paper markings are required
- How to mark E-mails on the classified network
- Marking requirements for CREM and classified parts

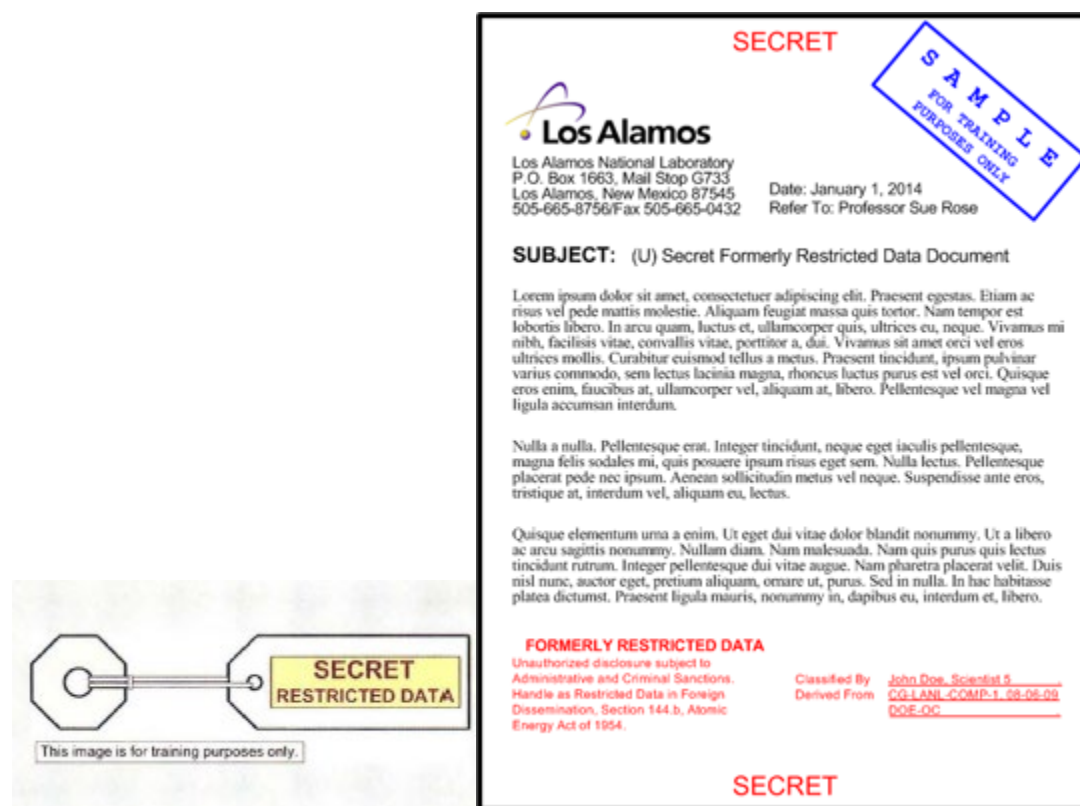
### Marking Classified Matter



- Prior to April 1, 1996 - matter need to only contain level and category if RD or FRD for proper protection.
- After April 1, 1996 - matter must be marked in accordance with the CMPC Handbook.

Regardless of its date or agency of origin, classified matter must be marked to indicate at least the classification level and category if Restricted Data or Formerly Restricted Data to ensure proper protection. Documents generated and marked before April 1st, 1996 are not required to be remarked to comply with the Classified Matter Protection and Control (CMPC) Handbook while being stored at LANL. However, all classified matter must be reviewed and brought up to current marking standards identified in the CMPC Handbook whenever it is released from LANL or by current holder or removed from a state of permanent storage and placed into use.


## Derivative Classifier (DC) Review



The originator of any matter that may be classified, including all matter that is prepared in a classified subject area, must ensure the matter is reviewed for classification by a Derivative Classifier (DC). Prior to classification review, matter that may be classified must be protected at the highest potential classification level and category.



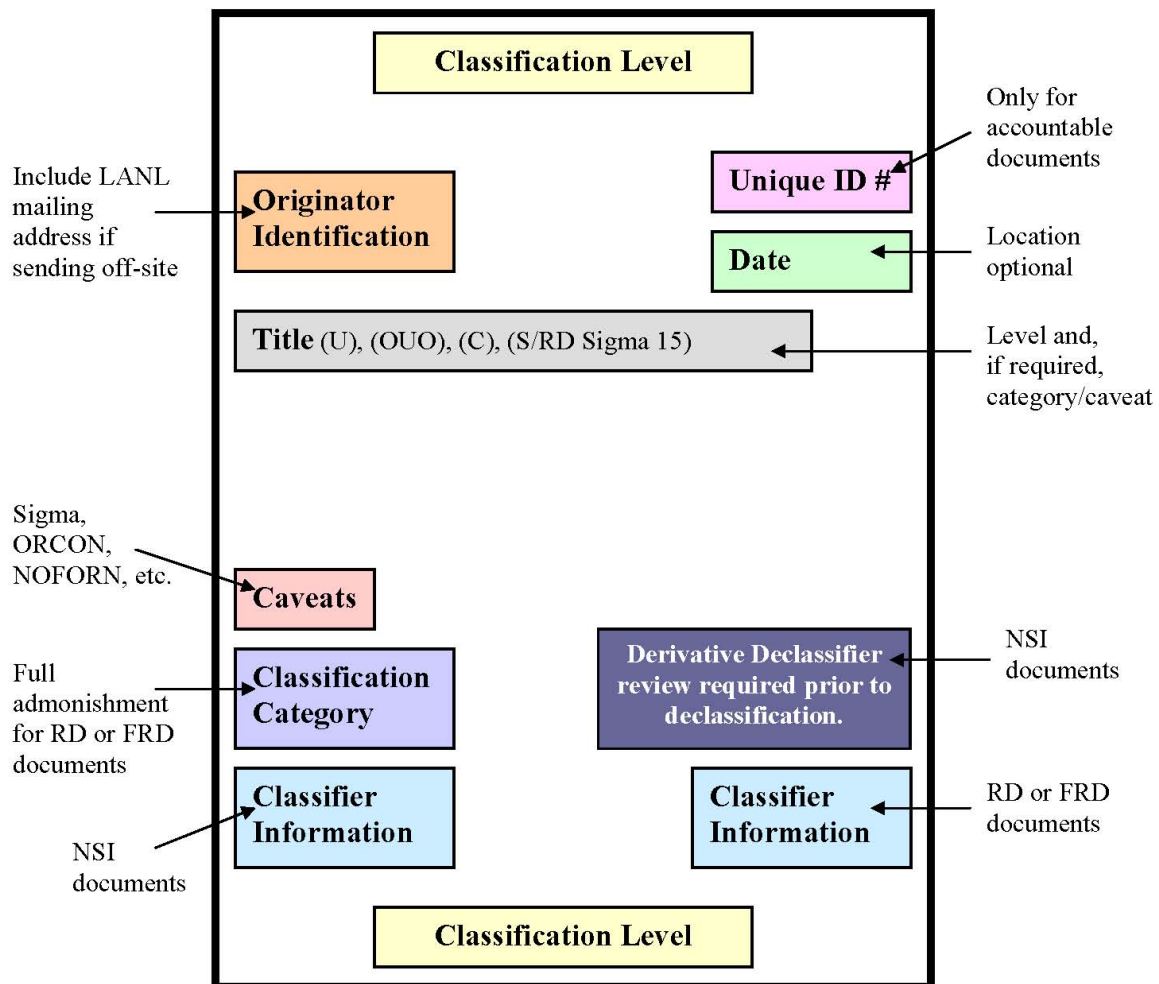
# Marking Classified Documents and Parts

|  |  |
|--|--|
| <b>SECRET</b>  |  |
| <br>Los Alamos National Laboratory<br>P.O. Box 1663, Mail Stop G733<br>Los Alamos, New Mexico 87545<br>505-665-8756/Fax 505-665-0432  | Date: January 1, 2014<br>Refer To: Professor Sue Rose  |
| <b>SAMPLE</b><br>FOR TRAINING<br>PURPOSES ONLY   |  |
| <b>SUBJECT: (U) Secret Restricted Data Document</b>  |  |
| <p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent egestas. Etiam ac risus vel pede mattis molestie. Aliquam feugiat massa quis tortor. Nam tempor est lobortis libero. In arcu quam, luctus et, ullamcorper quis, ultrices eu, neque. Vivamus mi nibbi, facilisis vitae, convallis vitae, porttitor a, dui. Vivamus sit amet orci vel eros ultrices mollis. Curabitur euismod tellus a metus. Praesent tincidunt, ipsum pulvinar varius commodo, sem lectus lacinia magna, rhoncus luctus purus est vel orci. Quisque eros enim, faucibus at, ullamcorper vel, aliquam at, libero. Pellentesque vel magna vel ligula accumsan interdum.</p> <p>Nulla a nulla. Pellentesque erat. Integer tincidunt, neque eget iaculis pellentesque, magna felis sodales mi, quis posuere ipsum risus eget sem. Nulla lectus. Pellentesque placerat pede nec ipsum. Aenean sollicitudin metus vel neque. Suspendisse ante eros, tristique at, interdum vel, aliquam eu, lectus.</p> <p>Quisque elementum urna a enim. Ut eget dui vitae dolor blandit nonummy. Ut a libero ac arcu sagittis nonummy. Nullam diam. Nam malesuada. Nam quis purus quis lectus tincidunt rutrum. Integer pellentesque dui vitae augue. Nam pharetra placerat velit. Duis nisl nunc, auctor eget, pretium aliquam, ornare ut, purus. Sed in nulla. In hac habitasse platea dictumst. Praesent ligula mauris, nonummy in, dapibus eu, interdum et, libero.</p> |  |
| <b>RESTRICTED DATA</b><br>This document contains Restricted Data as defined in the Atomic Energy Act of 1954, as amended. Unauthorized disclosure subject to Administrative and Criminal Sanctions.  | Classified By <u>John Doe, Scientist 5</u><br>Derived From <u>CG-LANL-COMP-1.08-06-00</u><br><u>DOE-OG</u> |
| <b>SECRET</b>  |  |

The originator of a newly created classified document must ensure each classified document is marked as required. Classification markings must be clearly distinguishable from the information text of the document. Markings may be a larger font size, a different color, or both to distinguish between information and text. A blank line may be placed between the classification-level marking and the information text.

When marking the level or category is not practical, written notification of the classification must be furnished to all recipients.

## Mandatory Markings - First Page of Text



- the highest classification level of the document at the top and bottom of the pages, and
- the category admonishment on the lower left-hand side of the pages if the document is Restricted Data (RD) or Formerly Restricted Data (FRD).

National Security Information (NSI) documents do not require a category admonishment marking.

The following markings are required on the first page of text and optional on any cover page or title page:

1. Date of preparation,
2. Originator identification,
3. Title or subject line with classification of title or subject immediately preceding the title,
4. Any applicable caveats or special handling requirements on the lower left-hand side of the page (above the category admonishment marking),
5. Category admonishment marking, and
6. Derivative classifier information must be on the lower right-hand side of the page if the document is RD or FRD.

If the document is NSI, the derivative classifier marking must be placed on the lower left-hand side of the page. If the document is accountable, a unique identification number must be on the first page of text, preferably located on the upper right-hand corner of the document.

As of February 25, 2008, all newly created NSI documents must include the following statement "Derivative Declassifier review required prior to declassification."

This new marking must also be applied to any NSI document dated after April 1, 1996, that is sent outside of LANL.

## Marking All Classified Documents - First Page of Text

**TOP SECRET**

**Los Alamos**  
Los Alamos National Laboratory  
P.O. Box 1663, Mail Stop C723  
Los Alamos, New Mexico 87545  
505-665-8796/Fax 505-665-0432

**12345678**

Date: January 1, 2010  
Refer To: Professor Sue Rose

**SAMPLE**  
FOR TRAINING  
PURPOSES ONLY

**SUBJECT:** (U) Top Secret National Security Information Document

(TS) Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent egetas. Etiam ac risus vel pede nunc molestie. Aliquam feugiat massa quis tortor. Nam tempus est lobortis libero. In arcu quam, lacus et, ullamcorper quis, ultrices eu, nunc. Vivamus nisi nibb, facilisis vitae, convallis vitae, purtitor a, dui. Vivamus sit amet orci vel eros ultrices mollis. Curabitur euismod tellus a metus. Praesent tincidunt, ipsum pulvisar variis commodo, sem lectus lacinia magna, rhoncus lectus purus est vel orci. Quisque eros enim, faucibus et, ullamcorper vel, aliquam ac, libero. Pellentesque vel magna vel ligula accumsan interdum.

(S) Nullo a nulla. Pellentesque erat. Integer tincidunt, neque eget inculis pellentesque, magna felis sociates mi, quis posuere ipsum risus eget sem. Nulla lectus. Pellentesque placerat pede nec ipsum. Aenean sollicitudin metus vel neque. Suspendisse ante eros, tristique ut, interdum vel, aliquam eu, lectus.

(U) Quisque elementum urna a enim. Ut eget dui vitae dolor blandit necummy. Ut a libero ac arcu sagittis necummy. Nullam diam. Nam molestiae. Nam quis purus quis lectus tincidunt rutrum. Integer pellentesque dui vitae nunc. Nam pharetra placerat velit. Duis nisl nunc, auctor eget, pretium aliquam, ornare ut, purus. Sed in nulla. In hac habitasse platea dictumst. Praesent ligula mauris, accummy in, dapibus eu, interdum et, libero.


Classified By: John Doe, Secretariat  
Derived From: COL-498, STOMP-1, DDE-11  
Declassify On: 2025, EY

Derivative Declassifier  
review required prior to  
declassification

**TOP SECRET**


All classified documents must identify the date of preparation and the originator identification on the first page of the document. When a classified document is sent outside the Laboratory, it must be marked with the name and mailing address of the organization responsible for preparing the classified document. It is recommended to mark all classified documents with the name and mailing address of the originator to preclude document corrections later. Printing the first page of the document on company letterhead is acceptable provided the letterhead contains all the required mailing address information. Accountable classified matter must have a unique identification number placed on the first page, preferably in the upper right corner.

## Subject and Titles

|   |  |
|---|--|
| <b>SECRET</b>   |  |
| <br><b>Los Alamos</b><br>Los Alamos National Laboratory<br>P.O. Box 1663, Mail Stop G733<br>Los Alamos, New Mexico 87545<br>505-665-8756/Fax 505-665-0432  | <b>DATE:</b> January 1, 2014<br><b>Refer To:</b> Professor Sue Rose  |
| <b>SUBJECT:</b> (U) Secret Restricted Data Document   |  |
| <p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent egestas. Etiam ac risus vel pede mattis molestie. Aliquam feugiat massa quis tortor. Nam tempor est lobortis libero. In arcu quam, luctus et, ullamcorper quis, ultrices eu, neque. Vivamus mi nibh, facilisis vitae, convallis vitae, porttitor a, dui. Vivamus sit amet orci vel eros ultrices mollis. Curabitur euismod tellus a metus. Praesent tincidunt, ipsum pulvinar varius commodo, sem lectus lacinia magna, rhoncus luctus purus est vel orci. Quisque eros enim, faucibus at, ullamcorper vel, aliquam at, libero. Pellentesque vel magna vel ligula accumsan interdum.</p> <p>Nulla a nulla. Pellentesque erat. Integer tincidunt, neque eget iaculis pellentesque, magna felis sodales mi, quis posuere ipsum risus eget sem. Nulla lectus. Pellentesque placerat pede nec ipsum. Aenean sollicitudin metus vel neque. Suspendisse ante eros, tristique at, interdum vel, aliquam eu, lectus.</p> <p>Quisque elementum urna a enim. Ut eget dui vitae dolor blandit nonummy. Ut a libero ac arcu sagittis nonummy. Nullam diam. Nam malesuada. Nam quis purus quis lectus tincidunt rutrum. Integer pellentesque dui vitae augue. Nam pharetra placerat velit. Duis nisl nunc, auctor eget, pretium aliquam, ornare ut, purus. Sed in nulla. In hac habitasse platea dictumst. Praesent ligula mauris, nonummy in, dapibus eu, interdum et, libero.</p> |  |
| <b>RESTRICTED DATA</b><br><small>This document contains Restricted Data as defined in the Atomic Energy Act of 1954, as amended. Unauthorized disclosure subject to Administrative and Criminal Sanctions.</small>  | <small>Classified By</small> <u>John Doe, Scientist 5</u><br><small>Derived From</small> <u>CG-LANL-COMP-1 08-08-09</u><br><u>DOE-OC</u> |
| <b>SECRET</b>   |  |

Except for extraordinary circumstances, documents must be assigned an unclassified title and marked to indicate such (e.g., U for unclassified, OOU for Official Use Only or UCNI for Unclassified Controlled Nuclear Information). If a classified title or subject is used, it must be marked with the appropriate classification level, category and caveats immediately preceding the title or subject. When classified documents with unmarked titles and/or subjects are sent outside of LANL or a multi-site work group, the titles and/or subjects must be reviewed by a DC or the Classification Group and then marked appropriately.

## Marking Caveats



Los Alamos National Laboratory  
P.O. Box 1663, Mail Stop G733  
Los Alamos, New Mexico 87545  
505-665-8756/Fax 505-665-0432

**SECRET**

Date: January 1, 2014  
Refer To: Professor Sue Rose

**SAMPLE**  
FOR TRAINING  
PURPOSES ONLY

**SUBJECT:** (U) Secret Restricted Data Document

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent egestas. Etiam ac risus vel pede mattis molestie. Aliquam feugiat massa quis tortor. Nam tempor est lobortis libero. In arcu quam, luctus et, ullamcorper quis, ultrices eu, neque. Vivamus mi nibh, facilisis vitae, convallis vitae, porttitor a, dui. Vivamus sit amet orci vel eros ultrices mollis. Curabitur euismod tellus a metus. Praesent tincidunt, ipsum pulvinar varius commodo, sem lectus lacinia magna, rhoncus luctus purus est vel orci. Quisque eros enim, faucibus at, ullamcorper vel, aliquam at, libero. Pellentesque vel magna vel ligula accumsan interdum.

Nulla a nulla. Pellentesque erat. Integer tincidunt, neque eget iaculis pellentesque, magna felis sodales mi, quis posuere ipsum risus eget sem. Nulla lectus. Pellentesque placerat pede nec ipsum. Aenean sollicitudin metus vel neque. Suspendisse ante eros, tristique at, interdum vel, aliquam eu, lectus.

Quisque elementum urna a enim. Ut eget dui vitae dolor blandit nonummy. Ut a libero ac arcu sagittis nonummy. Nullam diam. Nam malesuada. Nam quis purus quis lectus tincidunt rutrum. Integer pellentesque dui vitae augue. Nam pharetra placerat velit. Duis nisl nunc, auctor eget, pretium aliquam, ornare ut, purus. Sed in nulla. In hac habitasse platea dictumst. Praesent ligula mauris, nonummy in, dapibus eu, interdum et, libero.

**SIGMA 15**

**RESTRICTED DATA**

This document contains Restricted Data as defined in the Atomic Energy Act of 1954, as amended. Unauthorized disclosure subject to Administrative and Criminal Sanctions.


**SECRET**

Classified By John Doe, Scientist 5  
Derived From CG-LANL-COMP-1 08-06-09  
DOE-OC

Caveats are special handling or dissemination requirements. Some examples are: NOFORN - no foreign dissemination, ORCON- originator controlled, and Sigma Categories. Not all classified matter have caveats, but if they exist, a marking is located on the left-hand side of the document above the category marking on the cover page (if any), title page (if any) or first page of text.

# RD and FRD Classifier Marking

CONFIDENTIAL



Los Alamos National Laboratory  
P.O. Box 1663, Mail Stop G733  
Los Alamos, New Mexico 87545  
505-665-8756/Fax 505-665-0432

Date: January 1, 2014  
Refer To: Professor Sue Rose

SAMPLE  
FOR TRAINING  
PURPOSES ONLY

**SUBJECT:** (U) Confidential Restricted Data Document

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent egestas. Etiam ac risus vel pede mattis molestie. Aliquam feugiat massa quis toetor. Nam tempor est lobetis libero. In arcu quam, luctus et, ullamcorper quis, ultrices eu, neque. Vivamus mi nibb, facilisis vitae, convallis vitae, porttitor a, dui. Vivamus sit amet orci vel eros ultrices mollis. Curabitur euismod tellus a metus. Praesent tincidunt, ipsum pulvinar varius commodo, sem lectus lacinia magna, rhoncus luctus purus est vel orci. Quisque eros enim, faucibus at, ullamcorper vel, aliquam at, libero. Pellentesque vel magna vel ligula accumsan interdum.

Nulla a nulla. Pellentesque erat. Integer tincidunt, neque eget iaculis pellentesque, magna felis sodales mi, quis posuere ipsum risus eget sem. Nulla lectus. Pellentesque placerat pede nec ipsum. Aenean sollicitudin metus vel neque. Suspendisse ante eros, tristique at, interdum vel, aliquam eu, lectus.

Quisque elementum urna a enim. Ut eget dui vitae dolor blandit nonummy. Ut a libero ac arcu sagittis nonummy. Nullam diam. Nam malesuada. Nam quis purus quis lectus tincidunt rutrum. Integer pellentesque dui vitae augue. Nam pharetra placerat velit. Duis nisl nunc, auctor eget, pretium aliquam, ornare ut, purus. Sed in nulla. In hac habitasse platea dictumst. Praesent ligula mauris, nonummy in, dapibus eu, interdum et, libero.

**RESTRICTED DATA**


This document contains Restricted Data as defined in the Atomic Energy Act of 1954, as amended. Unauthorized disclosure is subject to Administrative and Criminal Sanctions.

Classified By John Doe, Scientist 5  
Derived From CG-LANI-COMP-1 08-05-09  
DOE-OC

CONFIDENTIAL

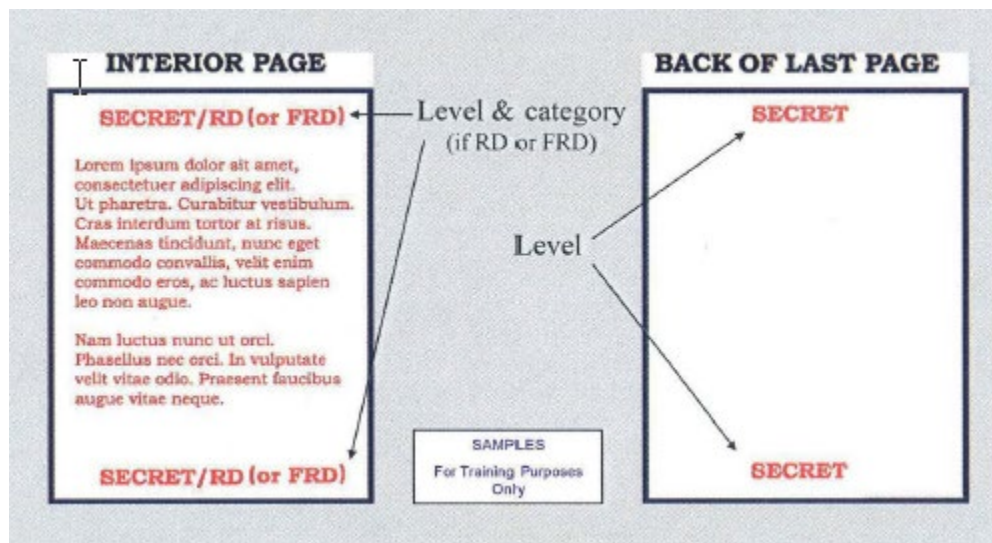
Classifier markings or stamp for RD and FRD documents must be placed on the lower right corner of the first page of text. No interior classifier markings are required.

## Marking NSI

|   |  |
|---|--|
| <b>SECRET</b>   |  |
| <br><b>Los Alamos</b><br>Los Alamos National Laboratory<br>P.O. Box 1663, Mail Stop G733<br>Los Alamos, New Mexico 87545<br>505-665-8756/Fax 505-665-0432  | <b>SAMPLE</b><br>FOR TRAINING<br>PURPOSES ONLY                                 |
| Date: January 1, 2014<br>Refer To: Professor Sue Rose   |  |
| <b>SUBJECT: (U) Secret National Security Information Document</b>   |  |
| <p><b>(S)</b> Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent egestas. Etiam ac risus vel pede mattis molestie. Aliquam feugiat massa quis tortor. Nam tempor est lobortis libero. In arcu quam, luctus et, ullamcorper quis, ultrices eu, neque. Vivamus mi nibbi, facilisis vitae, convallis vitae, porttitor a, dia. Vivamus sit amet orci vel eros ultrices mollis. Curabitur euismod tellus a metus. Praesent tincidunt, ipsum pulvinar varius commodo, sem lectus lacinia magna, rhoncus luctus purus est vel orci. Quisque eros enim, faucibus at, ullamcorper vel, aliquam at, libero. Pellentesque vel magna vel ligula accumsan interdum.</p> <p><b>(C)</b> Nulla a nulla. Pellentesque erat. Integer tincidunt, neque eget iaculis pellentesque, magna felis sodales mi, quis posuere ipsum risus eget sem. Nulla lectus. Pellentesque placerat pede nec ipsum. Aenean sollicitudin metus vel neque. Suspendisse ante eros, tristique at, interdum vel, aliquam eu, lectus.</p> <p><b>(U)</b> Quisque elementum urna a enim. Ut eget dui vitae dolor blandit nonummy. Ut a libero ac arcu sagittis nonummy. Nullam diam. Nam malesuada. Nam quis purus quis lectus tincidunt rutrum. Integer pellentesque dui vitae augue. Nam pharetra placerat velit. Duis nisl nunc, auctor eget, pretium aliquam, ornare ut, purus. Sed in nulla. In hac habitasse platea dictumst. Praesent ligula mauris, nonummy in, dapibus eu, interdum et, libero.</p> |  |
| Classified By <u>John Doe, Scientist 5</u><br>Derived From <u>CG-LANS-COMP-1, 08/09, DOE-CC,</u><br>Declassify On <u>25XX. Declassify when the information</u><br><u>is released by the cognizant entity</u>  | <b>Derivative Declassifier</b><br>review required prior to<br>declassification |
| <b>SECRET</b>   |  |

NSI documents do not require a full admonishment marking or stamp, on the first page or category markings on interior pages. The absence of this stamp actually indicates that it is NSI. However, classifier markings must be placed on the lower left corner of the first page of the document. Additionally, a new marking is required on the lower right of the document stating a derivative declassifier review is required prior to declassification. Thus, NSI documents are no longer allowed to be automatically declassified based on a date or event.

## Mandatory Marking - Interior Pages and Back of Last Page



Documents classified as RD and FRD with additional pages must have level and category marked on the top and bottom of subsequent pages. On the back side of the last page, the level must be marked on the top and bottom. You may use a back cover sheet if the back of the last page contains text. Good business practice suggests using the back cover sheet or a blank page marked with the level.

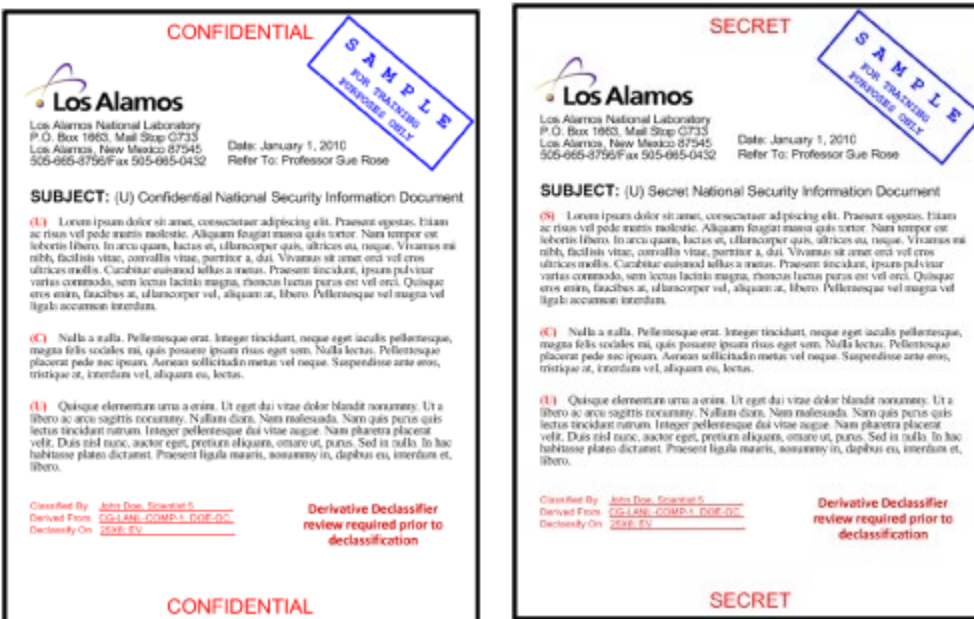
There are three acceptable ways to meet the requirements for marking the back of a classified document:

- A pre-printed routing slip or cover sheet, or
- A blank sheet of paper marked with the classification level, or
- The last page of the document marked with the classification level, provided that no text appears on the back of the last page.

The interior page category markings for RD and FRD documents are not required to be re-marked if the document was created before July 9, 1998.



## Portion Marking NSI Documents



NSI documents must be portion marked. Portion marking allows various sections of the same document to contain different levels of classification. Each section, part, paragraph, graphic, or figure on any NSI document or page change created after April 1, 1997, and are in use (i.e., not in approved storage) must be portion marked to show the classification level and applicable caveat, unclassified controlled (such as UCNI or OUO) or unclassified marking.

If any NSI document is sent outside of LANL by current holder or removed from a state of permanent storage and placed into use, the entire document must be portion marked. Portion markings may be typed or hand written. If the portion has a number, letter, or bullet, then the marking must be placed immediately preceding the portion to which they pertain but following the number, letter, or bullet of the portion.

## Marking Classified Working Papers/Drafts



- Date of origin - first page
- Classification level - top & bottom of cover page (if any), title page (if any), first page of text and back of last page
- Classification level (including unclassified) of each page - top & bottom of each interior page
- Classification category and full admonishment if RD or FRD, - first page
- The words DRAFT or WORKING PAPER - first page
- Applicable caveats - first page

## More on Classified Working Papers/Drafts

- Classified working papers must be protected
- Classified working papers must be destroyed when no longer needed

- Classified working papers must be protected in accordance with the assigned classification level and category. Classified working papers must be destroyed when no longer needed.

[illegible]

## Marking Classified E-mail Messages

Messages that have been reviewed for classification must be marked according to the results of the review.

## **Marking a Printed or Hard Copy Email Message or Attachment**

If the e-mail message or attachment is printed to a hard copy, the recipient must ensure it is marked as a final document.

## **Transmission of Classified E-mail Outside of LANL's Red Network**

When electronic files are transmitted outside of LANL's red network or multi-site work group, the sender must ensure the document is marked:

- As a final document
- According to current marking standards in the Classified Matter Protection and Control (CMPC) Handbook.

**Note:** A working group may include individuals or organizations outside the Laboratory.

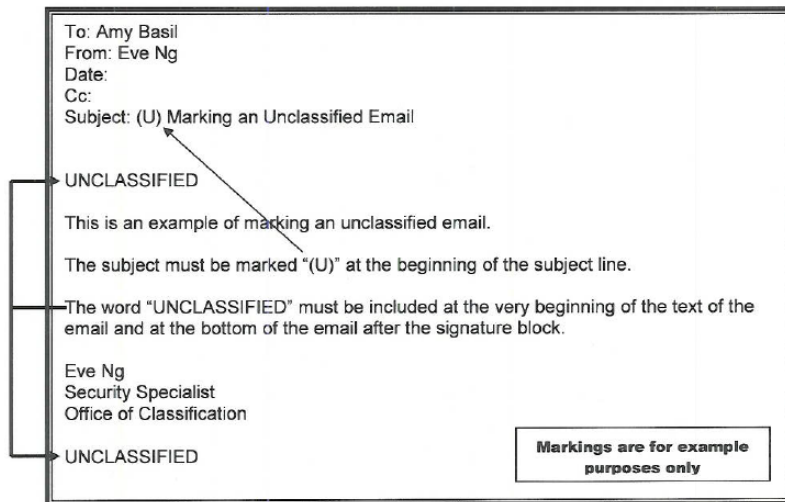
The Recipient Must:

- Verify that any printed copies contain appropriately applied markings,
- mark the back of the last page of each document with its classification level and category (if RD or FRD), and
- attach appropriate cover sheets.

### **Guidelines for Marking E-mail on a Classified Network**

- E-mails generated/created on a classified network must be marked as final documents.
- The following images demonstrate how to mark e-mails generated/created on a classified network.
- *Example One*

**MARKING EXAMPLE FOR AN EMAIL  
CONTAINING UNCLASSIFIED INFORMATION**



## **Guidelines for Marking E-mail on a Classified Network Continued**

*Example Two*

**MARKING EXAMPLE FOR A DERIVATIVELY CLASSIFIED EMAIL  
CONTAINING NATIONAL SECURITY INFORMATION**

To: Amy Basil  
From: Eve Ng  
Date:  
Cc:  
Subject: (U) Marking an Email Derivatively Classified as NSI

**SECRET**

(U) This is an example of marking an email that is derivatively classified as containing National Security Information.

(S) The subject line must be marked with the classification level of the information contained in the subject line, not the classification level of information contained in the overall email. In this example, the subject is unclassified.

--

(S) The overall classification level of the email must be included at the beginning of the text of the email and at the bottom after the special control marking.

(C) Since this email contains only NSI, each portion must be marked at its beginning with the highest classification level of the information contained in that portion.

(U) The 3-line classification authority block follows the signature block and must include all of the required information. It can be in block or linear form.

(U) The special control marking is placed after the classification authority block and before the overall classification level.

Eve Ng  
Security Specialist  
Office of Classification

Classified By: Eve Ng, Security Specialist  
Derived From: CG-XX-1, 9/1/2011, DOE OC  
Declassify On: 20280405

**OR**

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC; Declassify on: 20280405

Derivative Declassifier review  
required prior to declassification

**SECRET**

**Markings are for example  
purposes only**

## **Guidelines for Marking E-mail on a Classified Network Continued**

*Example Three*

**MARKING EXAMPLE FOR AN EMAIL  
CONTAINING RESTRICTED DATA INFORMATION**

To: Amy Basil  
From: Eve Ng  
Date:  
Cc:  
Subject: (U) Marking an Email Classified as RD

**SECRET//RESTRICTED DATA**

This is an example of marking an email containing Restricted Data information.

The subject line must be marked with the classification level and category (and any caveats, e.g., Sigma 14) of the information contained in the subject line, not the classification level and category (and caveats) of information contained in the overall email. In this example, the subject is unclassified.

The overall classification level and category (and caveats) of the email must be included at the beginning of the text of the email and at the bottom after the RD admonishment marking.

Since this email contains RD information, each portion is not required to be portion marked. If the email is portion marked, the classification level and category (e.g., S//RD) must be indicated for each portion that contains RD.

The 2-line classification authority block follows the signature block and must include all of the required information. It can be in block or linear form.

The RD admonishment marking is placed after the classification authority block and before the overall classification level and category marking.

Eve Ng  
Security Specialist  
Office of Classification

Classified By: Eve Ng, Security Specialist, OC  
Derived From: CG-XX-1, 9/1/2011, DOE OC

**OR**

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC

**RESTRICTED DATA**

This document contains RESTRICTED DATA  
as defined in the Atomic Energy Act of 1954.  
Unauthorized disclosure subject to administrative  
and criminal sanctions.

**SECRET//RESTRICTED DATA**

Markings are for example  
purposes only

## **Guidelines for Marking E-mail on a Classified Network Continued**

*Example Four*



**MARKING EXAMPLE FOR AN EMAIL  
CONTAINING FORMERLY RESTRICTED DATA INFORMATION**

To: Amy Basil  
From: Eve Ng  
Date:  
Cc:  
Subject: (U) Marking an Email Classified as FRD

**SECRET//FORMERLY RESTRICTED DATA**

This is an example of marking an email containing Formerly Restricted Data information.

The subject line must be marked with the classification level and category (and any caveats, e.g., Sigma 14) of the information contained in the subject line, not the classification level and category (and caveats) of information contained in the overall email. In this example, the subject is unclassified.

The overall classification level and category (and caveats) of the email must be included at the beginning of the text of the email and at the bottom after the FRD admonishment marking.

Since this email contains FRD information, each portion is not required to be portion marked. If the email is portion marked, the classification level and category (e.g., S//FRD) must be indicated for each portion that contains FRD.

The 2-line classification authority block follows the signature block and must include all of the required information. It can be in block or linear form.

The FRD admonishment marking is placed after the classification authority block and before the overall classification level and category marking.

Eve Ng  
Security Specialist  
Office of Classification

Classified By: Eve Ng, Security Specialist, OC  
Derived From: CG-XX-1, 9/1/2011, DOE OC

**OR**

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC

**FORMERLY RESTRICTED DATA**  
Unauthorized disclosure subject to administrative  
and criminal sanctions. Handle as RESTRICTED  
DATA in foreign dissemination. Section 144b, Atomic  
Energy Act of 1954.

**SECRET// FORMERLY RESTRICTED DATA**

**Markings are for example  
purposes only**

## **Guidelines for Marking E-mail on a Classified Network Continued**

*Example Five*



**MARKING EXAMPLE FOR A PORTION-MARKED EMAIL CONTAINING RESTRICTED DATA  
(OR FORMERLY RESTRICTED DATA) AND NATIONAL SECURITY INFORMATION**

NOTE: An email containing RD or FRD and NSI that is not portion-marked is marked following the example for an email containing only RD or FRD, as appropriate.

To: Amy Basil  
From: Eve Ng  
Date:  
Cc:  
Subject: (U) Marking a Portion-Marked Email Containing RD or FRD and NSI

SECRET//RESTRICTED DATA

(U) This is an example of marking a portion-marked email containing Restricted Data or Formerly Restricted Data and National Security Information.

(S//RD) The subject line must be marked with the classification level and category if RD or FRD (and any caveats, e.g., Sigma 14) of the information contained in the subject line, not the classification level and category of information contained in the overall email. In this example, the subject is unclassified.

(S) The overall classification level and category (and caveats) of the email must be included at the beginning of the text of the email and at the bottom after the source list.

(C) Since the originator decided to portion mark this email, each portion must be marked at its beginning with the highest classification level and category if RD or FRD (and caveats) of the information contained in that portion.

(U) The 3-line classification authority block follows the signature block and must include all of the required information, which for an email commingling RD or FRD and NSI has special rules. This marking can be in block or linear form.

(C//RD) The RD admonishment marking is placed after the classification authority block and before the source list

(C//RD) The source list containing the declassification instructions with the longest duration for each NSI source is placed immediately before the overall classification level and category marking at the bottom of the email.

Eve Ng  
Security Specialist  
Office of Classification

Classified By: Eve Ng, Security Specialist, OC  
Derived From: CG-XX-1, 9/1/2011, DOE OC  
Declassify On: N/A for RD portions; see source list for NSI portions

OR

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC; Declassify On: N/A for RD portions; see source list for NSI portions

RESTRICTED DATA

This document contains RESTRICTED DATA  
as defined in the Atomic Energy Act of 1954.  
Unauthorized disclosure subject to administrative  
and criminal sanctions.

Source List: CG-XX-1, 9/1/2011, DOE OC; Declassify On: 20201025

SECRET//RESTRICTED DATA

Markings are for example  
purposes only

## Guidelines for Marking E-mail on a Classified Network Continued

*Example Six*

**MARKING EXAMPLE FOR AN EMAIL CONTAINING  
ONLY TRANSClassIFIED FOREIGN NUCLEAR INFORMATION**

To: Amy Basil  
From: Eve Ng  
Date:  
Cc:  
Subject: (U) Marking an Email Classified as TFNI

**SECRET//TRANSClassIFIED FOREIGN NUCLEAR INFORMATION**

(C//TFNI) This is an example of marking an email containing Transclassified Foreign Nuclear Information.

(U) The subject line must be marked with the classification level and category of the information contained in the subject line, not the classification level and category of information contained in the overall email. In this example, the subject is unclassified.

(C//TFNI) The overall classification level and category of the email must be included at the beginning of the text of the email and at the bottom after the classification authority block.

(U) Since this email contains TFNI but not RD or FRD, each portion of the email must be marked at its beginning with the highest classification level and category of the information contained in that portion.

(S//TFNI) The 3-line classification authority block follows the signature block and must include all of the required information. It can be in block or linear form.

Eve Ng  
Security Specialist  
Office of Classification

Classified By: Eve Ng, Security Specialist, OC  
Derived From: CG-XX-1, 9/1/2011, DOE OC  
Declassify On: N/A to TFNI portions

**OR**

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC; Declassify On:  
N/A to TFNI portions

**SECRET//TRANSClassIFIED FOREIGN NUCLEAR INFORMATION**

**Markings are for example  
purposes only**

## **Guidelines for Marking E-mail on a Classified Network Continued**

*Example Seven*

**MARKING EXAMPLE FOR AN EMAIL CONTAINING  
NATIONAL SECURITY INFORMATION AND  
TRANSClassIFIED FOREIGN NUCLEAR INFORMATION**

To: Amy Basil  
From: Eve Ng  
Date:  
Cc:  
Subject: (U) Marking a Portion-Marked Email Containing NSI AND TFNI

**SECRET//TRANSClassIFIED FOREIGN NUCLEAR INFORMATION**

(U) This is an example of marking a portion-marked email containing National Security Information and Transclassified Foreign Nuclear Information.

(S//TFNI) The subject line must be marked with the classification level and category if TFNI of the information contained in the subject line, not the classification level and category of information contained in the overall email. In this example, the subject is unclassified.

(S//TFNI) The overall classification level and category of the email must be included at the beginning of the text of the EMAIL and at the bottom after the source list.

(C) Since this email contains both NSI and TFNI but no RD or FRD, each portion of the email must be marked at its beginning with the highest classification level and category of the information contained in that portion.

(U) The 3-line classification authority block follows the signature block and must include all of the required information, which for an email commingling NSI and TFNI has special rules. This marking can be in block or linear form.

(U) The special control marking is placed after the classification authority block.

(C) The source list containing the declassification instructions with the longest duration for each NSI source is placed immediately before the overall classification level and category marking.

Eve Ng  
Security Specialist  
Office of Classification

Classified By: Eve Ng, Security Specialist, OC  
Derived From: CG-XX-1, 9/1/2011, DOE OC  
Declassify On: N/A for TFNI portions; see source list for NSI portions

**OR**

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC; Declassify On: N/A for TFNI portions; see source list for NSI portions

Derivative Declassifier review  
required prior to declassification

Source List: CG-XX-1, 9/1/2011, DOE OC; Declassify On: 20201025

**SECRET//TRANSClassIFIED FOREIGN NUCLEAR INFORMATION**

**Markings are for example  
purposes only**

## **Guidelines for Marking E-mail on a Classified Network Continued**

*Example Seven*

**MARKING EXAMPLE FOR AN EMAIL CONTAINING  
NATIONAL SECURITY INFORMATION AND  
TRANSClassIFIED FOREIGN NUCLEAR INFORMATION**

To: Amy Basil  
From: Eve Ng  
Date:  
Cc:  
Subject: (U) Marking a Portion-Marked Email Containing NSI AND TFNI

**SECRET//TRANSClassIFIED FOREIGN NUCLEAR INFORMATION**

(U) This is an example of marking a portion-marked email containing National Security Information and Transclassified Foreign Nuclear Information.

(S//TFNI) The subject line must be marked with the classification level and category if TFNI of the information contained in the subject line, not the classification level and category of information contained in the overall email. In this example, the subject is unclassified.

(S//TFNI) The overall classification level and category of the email must be included at the beginning of the text of the EMAIL and at the bottom after the source list.

(C) Since this email contains both NSI and TFNI but no RD or FRD, each portion of the email must be marked at its beginning with the highest classification level and category of the information contained in that portion.

(U) The 3-line classification authority block follows the signature block and must include all of the required information, which for an email commingling NSI and TFNI has special rules. This marking can be in block or linear form.

(U) The special control marking is placed after the classification authority block.

(C) The source list containing the declassification instructions with the longest duration for each NSI source is placed immediately before the overall classification level and category marking.

Eve Ng  
Security Specialist  
Office of Classification

Classified By: Eve Ng, Security Specialist, OC  
Derived From: CG-XX-1, 9/1/2011, DOE OC  
Declassify On: N/A for TFNI portions; see source list for NSI portions

**OR**

Classified By: Eve Ng, Security Specialist, OC; Derived From: CG-XX-1, 9/1/2011, DOE OC; Declassify On: N/A for TFNI portions; see source list for NSI portions

Derivative Declassifier review  
required prior to declassification

Source List: CG-XX-1, 9/1/2011, DOE OC; Declassify On: 20201025

**SECRET//TRANSClassIFIED FOREIGN NUCLEAR INFORMATION**

**Markings are for example  
purposes only**

## **Guidelines for Marking E-mail on a Classified Network Continued**

*Example Eight*



**MARKING EXAMPLE FOR AN EMAIL CLASSIFIED  
USING MULTIPLE SOURCES**

To: Amy Basil  
From: Eve Ng  
Date:  
Cc:  
Subject: (U) Marking an Email Classified using Multiple Sources

**SECRET**

(U) This is an example of marking an email that was classified using multiple sources.

(S) The subject line must be marked with the classification level (and category, if RD or FRD) of the information contained in the subject line, not the classification level of information contained in the overall email. In this example, the subject is unclassified.

(S) The overall classification level (and category if RD or FRD) of the email must be included at the beginning of the text of the email and at the bottom after the source list.

(C) Since this email contains only NSI, each portion of the document must be marked at its beginning with the highest classification level of the information contained in that portion.

(U) The appropriate classification authority block follows the signature block and must include all of the required information. It can be in block or linear form.

(U) When the classification of an email is based on multiple sources, the entry for the "Derived From" line of the classification authority block is "Multiple Sources." For an email containing only NSI like this one, the entry on the "Declassify On" line reflects the longest duration of classification from all these sources.

(U) Since this email contains only NSI, the special control marking is placed after the classification authority block.

(U) A list of the source documents must be placed at the bottom of the email immediately before the overall classification level (and category if RD or FRD).

Eve Ng  
Security Specialist  
Office of Classification

Classified By: Eve Ng, Security Specialist  
Derived From: Multiple Sources  
Declassify On: 20280405

Derivative Declassifier review  
required prior to declassification

Source Document List:  
CG-XX-1, 9/10/10, DOE OC  
CG-ZZ-3, 11/12/12, DOE OC

**SECRET**

**Markings are for example  
purposes only**

## **Guidelines for Marking E-mail on a Classified Network Continued**

*Example Nine*

**MARKING EXAMPLE FOR A CLASSIFIED EMAIL  
TRANSMITTING A CLASSIFIED ATTACHMENT**

To: Amy Basil  
From: Eve Ng  
Date:  
Cc:  
Subject: (U) Marking an Email Classified as NSI with an SRD Attachment

SECRET//RESTRICTED DATA

Attachment contains SECRET//RESTRICTED DATA  
When separated from attachment, this email is SECRET.

(U) This is an example of marking an email that contains NSI with an RD attachment.

(U) The subject line must be marked with the classification level (and category if RD or FRD) of the information contained in the subject line, not the classification level of information contained in the overall email or attachment. In this example, the subject is unclassified.

(U) The overall classification level (and category if RD or FRD) of the email itself and its attachments must be included at the beginning of the text and at the bottom of the email. Immediately following the overall classification level (and category if RD or FRD) at the beginning of the text, the highest level (and category if RD or FRD) of the attachment must be identified.

(U) Wherever the attachment is shown (at the bottom of the email, elsewhere in the email, or in the attachment line), the classification level (and category if RD or FRD) of the information contained in the attachment must be indicated (e.g., SRD Attachment).

(U) The attachment must be marked correctly as a stand-alone document.

(S) Since this email is classified as NSI, it is portion marked, the 3-line classification authority block is used, and the special control marking is placed after the classification authority block. The "Derived From" line must include the sources used to classify the email. The "Declassify On" line should contain the declassification instruction for the email.

Eve Ng  
Security Specialist  
Office of Classification

Classified By: Eve Ng, Security Specialist  
Derived From: CG-XX-1, 9/1/2011, DOE OC  
Declassify On: 20280101

Derivative Declassifier review  
required prior to declassification

SECRET//RESTRICTED DATA



SRD Attachment

Markings are for example  
purposes only

## Guidelines for Marking E-mail on a Classified Network Continued

*Example Ten*

**MARKING EXAMPLE FOR AN UNCLASSIFIED  
EMAIL TRANSMITTING A CLASSIFIED ATTACHMENT**

To: Amy Basil  
From: Eve Ng  
Date:  
Cc:  
Subject: (U) Marking an Unclassified Email with a Classified Attachment

**SECRET**

Attachment contains **SECRET**  
When separated from attachment, this email is unclassified.

This is an example of marking an email that contains only unclassified information but transmits a classified attachment.

The subject line must be marked with the classification level and category of the information contained in the subject line, not the classification level and category of information contained in the overall email or attachment. In this example, the subject is unclassified.

The overall classification level (and category if RD or FRD) of the email itself and its attachments must be included at the beginning of the text and at the bottom of the email. Immediately following the overall classification level (and category if RD or FRD) at the beginning of the text, the highest level (and category) of the attachment(s) must be identified and followed by this statement: "When separated from attachment, this email is unclassified."

Wherever the attachment is shown (at the bottom of the email, elsewhere in the email, or in the attachment line), the classification level (and category if RD or FRD) of the information contained in the attachment must be indicated (e.g., **SRD Attachment**).

The attachment must be marked correctly as a stand-alone NSI document.

Since this email is unclassified, it is not portion marked and needs no classification authority block.

Eve Ng  
Security Specialist  
Office of Classification

**SECRET**



**Secret**  
**Attachment**

**Markings are for example  
purposes only**

## **Guidelines for Marking E-mail on a Classified Network Continued**

*Example Eleven*

#### MARKING EXAMPLE FOR A STRING OF CLASSIFIED EMAIL

To: Eve Ng  
From: Amy Basil  
Date: Friday, May 24, 2013 10:16 AM  
Subject: Re: (U) Marking a String of Emails

SECRET

(U) If you respond to or forward a classified email, you must review and classify the entire string, considering each section in the context of the entire email for classification.

(S) The overall classification level (and category if RD or FRD) of the string is included at the beginning of the text of your email and at the end of the entire string of emails. In this example, the first email is Confidential and the second is Secret, so the string has an overall classification level of Secret.

(C) The classification authority block is placed at the end of the string just before the overall classification level (and category if RD or FRD).

(C) Do not repeat the special control marking or any RD/FRD admonishment for your reply. However, you must carry forward any statements concerning classified attachments to the email string (e.g., "Attachment contains SECRET". When separated from attachment, this email is...). This should be placed at the top of the email string and below the overall classification level (and category if RD or FRD).

(U) For your classification authority block, the "Derived From" line should include all sources used to classify the entire email string. At a minimum, this should include any guide used to make your classification determination and any of the previous email. If a source from the previous email is used, this may be noted with "and email above". If there is a source list, it should be included at the end of the email string above the overall classification. The "Declassify On" line must reflect the longest duration of classification from all the sources for the entire string.

Amy Basil  
Security Specialist

SECRET

---

To: Basil, Amy  
From: Ng, Eve (HS)  
Date: Thursday, May 23, 2013 4:44 PM  
Subject: (U) Marking a String of Emails

CONFIDENTIAL

(C) The initial email is marked according to the classification of the information contained in the email. This email contains Confidential NSI.

Classified By: Eve Ng, Security Specialist  
Derived From: CG-XX-1, 9/1/2011, DOE OC  
Declassify On: 20280405

Derivative Declassifier review  
required prior to declassification

CONFIDENTIAL

Classified By: Amy Basil, Security Specialist, HS-61  
Derived From: CG-YY-1, 9/1/2011; DOE OC and email above  
Declassify On: 20280405

SECRET

Markings are for example  
purposes only

## Guidelines for Marking E-mail on a Classified Network Continued

*Example Twelve*



**APPENDIX B**  
**MARKING EXAMPLE FOR AN ORIGINALLY CLASSIFIED EMAIL**  
**CONTAINING NSI**

NOTE: This example is included for completeness. Original classification should only be done by a Federal employee with original classification authority whose training is up to date.

To: Eve Ng  
From: John Sobieski  
Date:  
Cc:  
Subject: (U) Marking an Email Originally Classified as NSI

SECRET

(U) This is an example of marking an email containing information considered to be National Security Information that is not adequately covered by existing guidance. Only an Original Classifier may do this initial classification. Remember that Restricted Data, Transclassified Foreign Nuclear Information, and Formerly Restricted Data are NEVER initially classified by an Original Classifier.

(S) The subject line must be marked with the classification level of the information contained in the subject line, not the classification level of information contained in the overall email. In this example, the subject is unclassified.

(S) The overall classification level of the email must be included at the beginning of the text of the email and at the bottom after the special control marking.

(C) Since this email contains only NSI, each portion must be marked at its beginning with the highest classification level of the information contained in that portion.

(C) The 3-line classification authority block follows the signature block and must include all of the required information. It can be in block or linear form. Rather than listing a guide that the decision is derived from, Original Classifiers must give the "Reason" for classification found in Section 1.4 of Executive Order 13526. This section describes the types of information that may be originally classified.

(S) Another difference is that an Original Classifier must establish a specific date or event for declassification based on the duration of the national security sensitivity of the information. Generally, this is 10 years from the date of the original decision unless the sensitivity of the information requires that it be classified for up to 25 years from the date of the original decision.

(C) The "Classified By" line may contain the Original Classifier's name and position OR his/her personal identifier.

(U) The special control marking is placed after the classification authority block and before the overall classification level.

John Sobieski  
Director, Examples Division  
Office of Classification

Classified By: John Sobieski, Director, Examples Division, OC OR ID# 55500  
Reason: 1.4(c)  
Declassify On: 20240202



OR

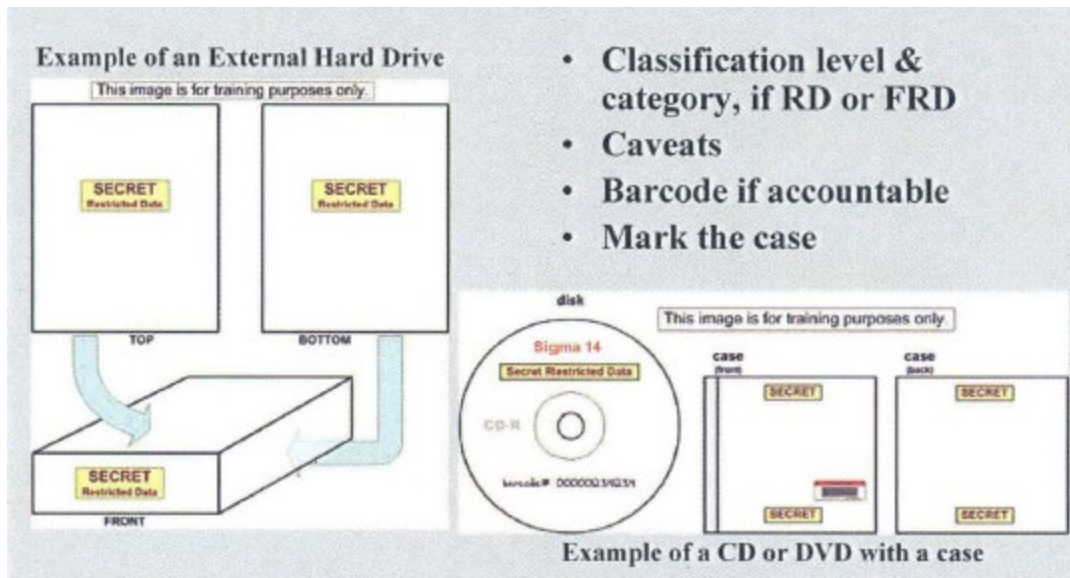
Classified By: John Sobieski, Director, Examples Division, OC Reason: 1.4(c); Declassify On: 20240202

Derivative Declassifier review  
required prior to declassification

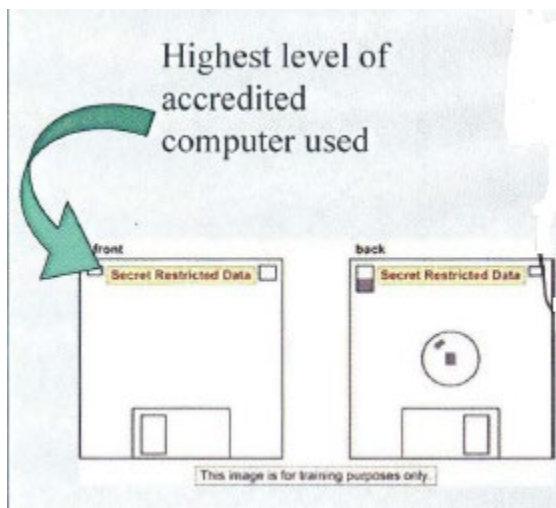
Markings are for example  
purposes only

SECRET

## Marking CREM



All classified removable electronic media (CREM) must be marked and protected at the highest level and category the classified computer system is accredited to process. The classification level and category, if RD or FRD, must be marked on the front and back of each piece of CREM. Applicable caveats must be marked on the front of each piece of CREM. If the CREM is accountable, it requires a barcode. Classification labels may be used to mark CREM; however, if the label impedes the operation of the media, alternative marking methods, such as marking with a Sharpie pen or any indelible ink, may be used. The classification level must be marked on the top and bottom of the front and back of any jewel case, box or cover holding CREM.



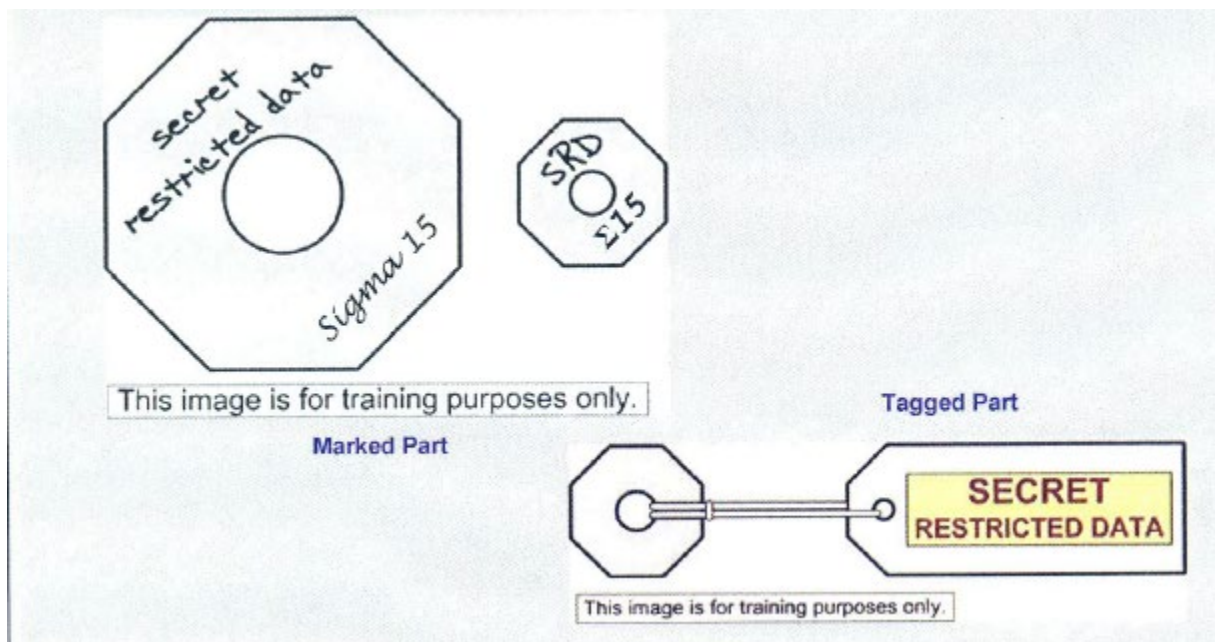
### Protect, mark, and handle CREM correctly!

- Media inserted in a "read/write" drive, even if no information was copied to it, must be protected, marked, and handled as CREM.

- Media inserted into a "read-only" drive of a classified computer do not need to be marked as classified.

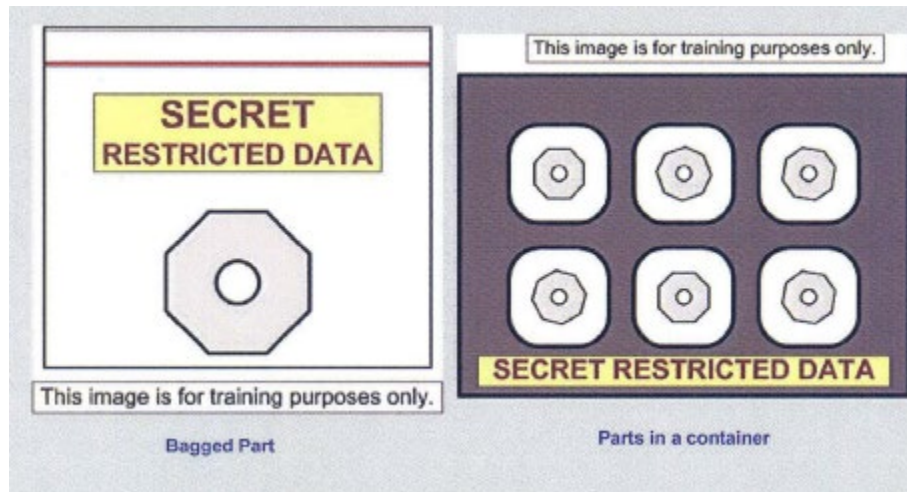
If a piece of CREM is produced, the person who produces it must protect, mark and handle it correctly. The CREM must be marked at the highest level and category, if RD or FRD, of the accredited computer used to produce it. This is true even if a CD or DVD is inserted into the "read/write" drive of a classified computer and no information was copied to the disc. Discs inserted into the "read-only" drive of a classified computer do NOT need to be marked as classified.

## Marking Classified Parts



The marking requirements for a classified part are different than the marking requirements for a document. The classification level, category, if RD or FRD, and applicable caveats must be conspicuously marked on the classified part, if possible, by any of the following methods: stamped, printed, etched, written, engraved or painted on the part. If these standard marking methods are not achievable, the markings must be affixed with a tag, sticker, decal or similar

method. Classifier information and origination date are maintained on the drawing specifications and are not required on each part.



If program requirements preclude markings on the parts or the parts are too small to adhere to these marking requirements, the classified part must be placed in a bag, box or container and the markings placed on the bag, box or container.

## Objective 6: Identify Reproduction Requirements

- Authorization requirements for reproducing classified documents
- Requirements for reproduction machines used to reproduce classified documents

In this section we will identify the authorization requirements for reproducing classified documents as well as requirements for reproduction machines used to reproduce classified documents.

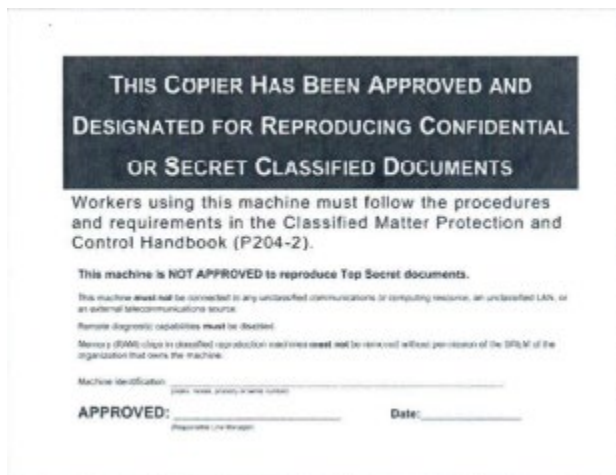
## Clearance and Need-to-Know



Accountable classified documents must only be reproduced by the accountable library Classified Matter Custodian (CMC).

Classified documents may be reproduced **ONLY** by people who have the proper clearance level and need-to-know in the performance of official duties. Accountable classified documents must only be reproduced by the accountable library CMCs.

## Copy Machines



Reproduce classified documents **ONLY** on machines approved for classified copying!

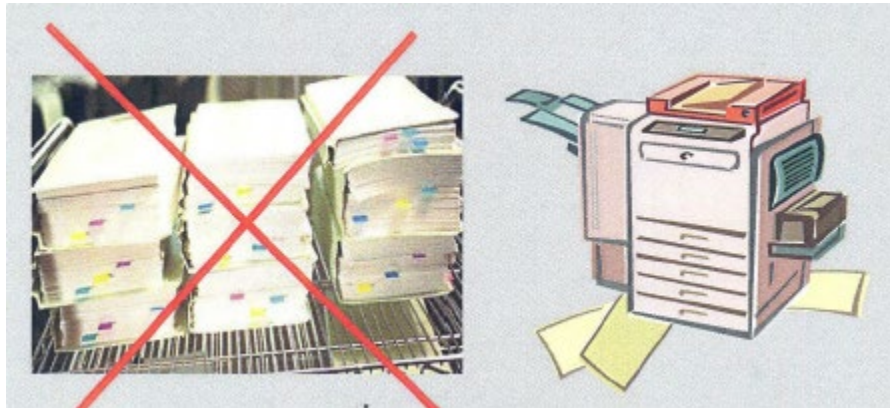
*Look for placard posted on or near the classified reproduction machine.*

Classified documents may be reproduced only using machines that are approved for classified copying. An authorized placard for classified copiers must be posted on or near the reproduction



machine affirming that the copier may indeed be used to copy classified matter. Reproduction machines used to duplicate classified matter must be located within a Limited Area or higher.

## Sanitization Procedure



The picture on the left shows an example of stacks of reproduced copies. Keep the number of copies to a minimum. The picture on the right shows pages of paper that may have fallen to the floor or behind the copy machine. Make sure that you have all of your pages before you leave the room.

Check for any caveats related to reproduction, and limit the number of copies you make. All copies of the classified document are classified as well and must be handled and protected accordingly. After copying classified, the machine must be sanitized. If a machine is analog, run three blank pages using the same copying process, e.g., double-sided, collated, etc., and destroy the blank pages as classified documents.

If the machine is digital, power the machine down for approximately 30 seconds or longer.

If a digital machine has an immediate image overwrite security feature enabled to automatically overwrite data after every job, then the machine does not have to be powered down. If the copy machine cannot be identified as analog or digital, both steps of running three blank pages and powering down the machine must be completed to sanitize the machine of residual images. Double-check the copier to ensure that the classified originals or copies are not left behind.

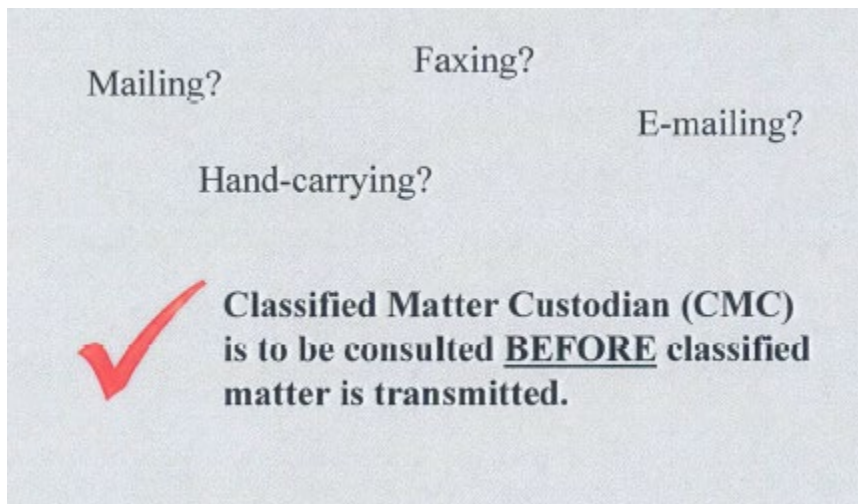
## Objective 7: Identify Transmission Requirements

- General requirements for transmitting classified matter

- Conditions requiring a receipt for transmittal
- Proper packaging to transmit classified matter
- Procedures for transmitting classified matter via:
  - hand-carrying within LANL (within and between security areas)
  - hand-carrying outside of LANL (off-site)
  - Fax
  - E-mail

In this section we will identify general requirements for transmitting classified matter, conditions requiring a receipt for transmittal of classified matter and the procedures for packaging and transmitting classified matter via hand-carrying within and outside of the Laboratory, as well as faxing and E-mailing.

## CMC Guidance



Classified matter can be safely and securely transmitted in a variety of ways, including mailing, hand-carrying, faxing and E-mailing by secure means. Classified matter can only be sent to approved classified mailing addresses. The Classified Matter Custodian is responsible for knowing the latest procedures and restrictions. It is best to consult with your CMC before transmitting classified information.

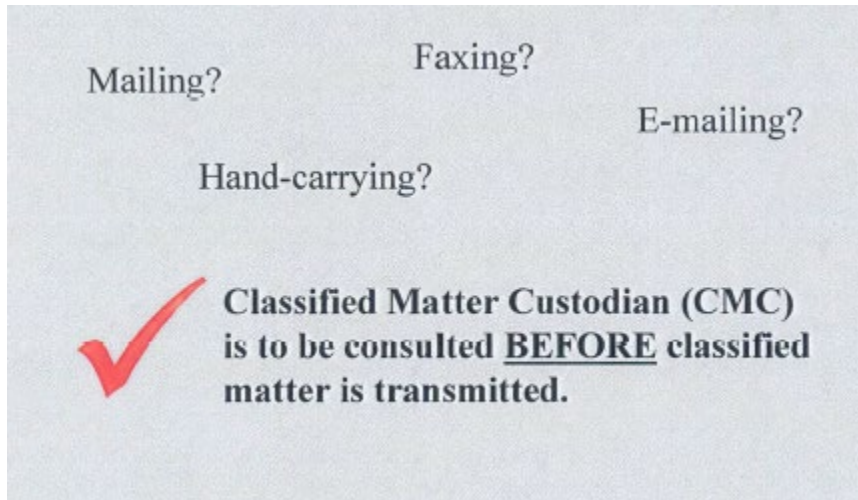
## General Requirements for Transmitting Classified Matter

Classified matter must be transmitted only in performance of official and contractual duties. Before transmitting classified matter workers must verify:

- the intended recipient's clearance, equivalent access authorization ( security clearance) relevant access;
- approvals, for example, sigma authorities;
- need-to-know for the matter being transmitted; and
- approved classified mail address.

Workers must ensure classified matter is marked in accordance with the requirements in the CMPC Handbook before it is transmitted outside of LANL or to a multi-site work group.

## CMC Guidance



Classified matter can be safely and securely transmitted in a variety of ways, including mailing, hand-carrying, faxing and E-mailing by secure means. Classified matter can only be sent to approved classified mailing addresses. The Classified Matter Custodian is responsible for knowing the latest procedures and restrictions. It is best to consult with your CMC before transmitting classified information.

## General Requirements for Transmitting Classified Matter

Classified matter must be transmitted only in performance of official and contractual duties. Before transmitting classified matter workers must verify:

- the intended recipient's clearance, equivalent access authorization ( security clearance) relevant access;
- approvals, for example, sigma authorities;
- need-to-know for the matter being transmitted; and
- approved classified mail address.

Workers must ensure classified matter is marked in accordance with the requirements in the CMPC Handbook before it is transmitted outside of LANL or to a multi-site work group.

## Proper Packaging to Transmit Classified Matter

- Consult with your CMC
  - Internal (within LANL) mailing of classified only requires a single wrap
  - External (outside LANL) mailing of classified requires double wrapping



- Hand-carrying within a security area requires only a cover sheet
- Hand-carrying between security areas requires single wrap
- Hand-carrying off-site ("off the hill") requires double wrap, completion of LANL form 1658, and a contingency plan
- Note: Rules are a little different for Top Secret matter. Consult with your CMC and/or the CMPC Handbook for transmitting Top Secret matter.

To properly package classified matter for transmission, it is best to consult with your CMC as there are different requirements based on the transmission method chosen. The CMC may be required to provide the supplies necessary to properly package classified matter. Your CMC will also verify a classified mailing address for the recipient in the LANL Mail Channel.

If you do not have a CMC, send email to the CMPC Team at [cmpe@lanl.gov](mailto:cmpe@lanl.gov) for assistance. To verify a classified mail address, send an email to [mailchannel@lanl.gov](mailto:mailchannel@lanl.gov).

## Hand-Carrying Classified Matter Within the Laboratory: within a Security Area

| Step | Action   |
|------|--|
| 1.   | Make sure the classified matter is marked appropriately.             |
| 2.   | Place cover sheets on the document.                                  |
| 3.   | Travel directly to the recipient's location without making any stops |
| 4.   | Verify the recipient's clearance and need-to-know.                   |
| 5.   | Ensure the recipient signs the receipt, if required                  |

Use this procedure for hand-carrying classified **within a security area**. If you are going outside of a building within the security area, consider the good business practice of using a carry-bag or marked envelope.

## Clarification - Scenario

If you were a resident of a TA-03, Building 1400 (NNSB) carrying classified matter to TA-03, Building 2327 (SCC) you may consider the good business practice of using a carry-bag or marked envelope.

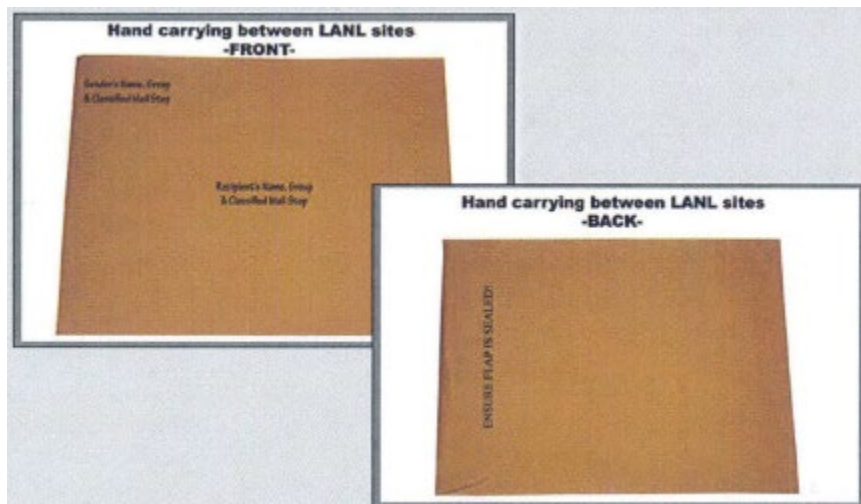
## Hand-Carrying Within the Laboratory: Between Security Areas

| Step | Action   |
|------|--|
| 1.   | Make sure the classified matter is marked appropriately. |

|    |   |
|----|---|
| 2. | Place cover sheets on the document.   |
| 3. | Place document in opaque envelope   |
| 4. | Seal envelope, if used; briefcase, if used; or locked bag, if used.                                       |
| 5. | Write sender's name, organization and classified mail stop on the left hand corner of the envelope.       |
| 6. | Write recipient's name, organization and classified mail stop in the center of the front of the envelope. |
| 7. | Travel directly to the recipient's location without making any stops.                                     |
| 8. | Verify the recipient's clearance and need-to-know.  |
| 9. | Ensure the recipient signs the receipt, if required.  |

Many employees believe that classified matter must be double-wrapped when hand-carrying between Laboratory sites. This is not required. Single wrapping is permitted when hand-carrying a classified document between security areas. Use this procedure to hand-carry within the Laboratory **between security areas**.

## Correctly Marked Envelopes for Hand-Carrying



This classified package is correctly marked for hand-carrying between security areas at the Laboratory.

## Clarification - Scenario

If you are a resident of TA-55 carrying classified matter to a building at TA-16 you would use a briefcase, marked envelope, or locked bag.

## Hand-carrying Outside of LANL (off-site)

- This transmission practice is highly discouraged
- Classified matter must be properly marked and double-wrapped
- Using a locked briefcase does not count as the outer wrapper when aboard public transportation
- Do not use fabric bags for hand-carrying off-site
- Use a receipt when transmitting Secret or Accountable matter
- Do not take your classified matter to unapproved facilities or private residences

Hand-carrying classified matter off-site is highly discouraged. All other means of transmission should be considered before reverting to hand-carrying off-site. Classified matter must be properly marked and double-wrapped in opaque material, as if it were going to be mailed off-site. A locked briefcase cannot serve as an outer wrapper when aboard public transportation, but can be used to carry the double-wrapped package. Reusable fabric bags with key locks are not permitted for hand-carrying classified matter outside of the Laboratory, except for deployable operations such as the Nuclear Emergency Search Team or Accident Response Group. A classified matter receipt must be used when transmitting Secret or Accountable matter. Do not remove your classified matter from approved storage facilities to private residences or other unapproved places such as hotel rooms in connection with your travel.

## Hand-carrying Outside of LANL (off-site), Continued

| Step | Actions   |
|------|---|
| 1.   | Complete LANL Form 1658, <i>"Certification and Approval to Hand Carry classified Matter Off-site"</i> for each instance of hand-carrying.             |
| 2.   | Develop a contingency plan for delayed arrival for each instance of hand-carrying.  |
| 3.   | Complete LANL Form 1655, <i>"Letter of Authorization to request alternative Airport Screening,"</i> if necessary, for each instance of hand-carrying. |
| 4.   | Ensure classified matter is appropriately packaged.   |
| 5.   | Prepare a classified matter receipt, if required.   |
| 6.   | Obtain manager approval on the LANL forms for each instance of hand-carrying.   |
| 7.   | Notify Security of intent to hand-carry classified by distributing the approved LANL forms <b>prior</b> to departure of travel.                       |

Use this procedure for hand-carrying classified off-site. This procedure must be followed for EACH instance of hand-carrying. Approvals to hand-carry off-site are no longer valid for one year. Distribution of the approved documents, as identified on the LANL forms, must also take place prior to departure of travel.

## **Faxing a Classified Document**

- Must be sent to and from a classified fax machine.
- Fax machine must be attended at all times.
- Sender is responsible for making sure the recipient has proper clearance, need-to-know, and authorities before sending fax.
- Include a receipt in the Fax transmission for all Accountable and Secret matter.

Faxing a classified document is permissible if it is sent to and from an approved classified facsimile (fax) and the fax machine is attended at all times. It is the responsibility of the sender to make sure that the recipient has the proper clearance, need-to-know, and authorities before sending the fax. When transmitting accountable or secret level matter, remember to include a receipt in the fax transmission. Request the recipient to immediately sign the receipt and fax it back.

## **E-mailing**

Before E-mailing information, ask yourself these questions:

- Are sending and receiving computers approved for classified transmission?
- Does the recipient have appropriate access authorization, any required formal access approval and need-to-know?
- Does the message and attachments, if any, contain all required classification markings?

E-mail may be used to transmit classified information and documents. Before information is E-mailed, you must ensure that the computers sending and receiving the information are approved for classified transmissions at the proper level and category. The sender is responsible for ensuring the recipient has the appropriate access authorization, any required formal access approval and need-to-know. Additionally, the sender must ensure the E-mail message and any attachments are appropriately marked.

## **Objective 8: Identify Destruction Requirements**

- Conditions requiring classified matter to be destroyed
- Steps required to destroy classified matter
- Requirements for inspection of destroyed classified matter
- Special procedures for destroying classified parts and accountable matter

In this section we will identify the conditions requiring classified matter to be destroyed, the procedures for destroying classified matter and the requirements for inspection of the classified matter once it is destroyed. We will also cover the special procedures for destroying classified parts and accountable matter.

# General Destruction Requirements

Classified matter must be destroyed when:

- No longer needed
- Multiple copies are found
- The document or material is obsolete
- At the conclusion of off-site meetings if the material is not to be used again

Inspect shredder residue to ensure it meets requirements each time destruction is completed.

In general, workers must destroy unneeded, multiple copies or obsolete classified matter and classified waste as soon as practical to reduce volume to the minimum necessary. All classified matter must be destroyed beyond recognition and must not permit subsequent recovery of classified information. However, classified matter covered by any current moratorium or court order must not be destroyed. Each time destruction of classified matter is completed, you must inspect the residue output to ensure that it meets the requirements.

## Crosscut Shredder



The Laboratory has approved certain types of destruction equipment located within security areas that may be used to destroy classified matter. The most common classified destruction equipment is the crosscut shredder with an output residue of 1 millimeter by 5 millimeters. Machines purchased and approved for classified use before December 31, 2003 that produce residue with the particle size not exceeding 1/32nd inch in width by 1/2 inch in length may continue to be used for the destruction of classified paper matter and non-paper products, except

microfilms, until equipment repair cannot restore the shredder to cut residue within the 1/32nd inch by 1/2 inch particle size. To determine if a shredder is approved for classified, look for the red and yellow approval sticker on the machine. If the sticker is not present, the machine cannot be used for destroying classified matter.

## Destroying Non-accountable Classified Documents

Los Alamos  
NATIONAL LABORATORY  
UNCLASSIFIED 8/17/19

Form 1704  
Certificate of Records Destruction  
Document Control and Records Management

DCRM USE ONLY  
Field Destruction ID

NOTE: All information on this form is used as a record of destruction for record material, which can include classified matter. All information on this form must be UNCLASSIFIED.

Section 1: Records Information (To be filled out by Requestor)

Office of Record (Org-Group) Requestor Z # Requestor Name Email

Example Formats: FA (SUD, SAFE, IP), HR (B), See LANL Organizations.

Use the plus and minus buttons to add or remove fields depending on the number of boxes needed.

| Description (Identify records to be destroyed with a detailed description. No classified terms) | DOE Retention Schedule | Classification Code | Earliest Record Date | Latest Record Date |
|---|------------------------|---------------------|----------------------|--------------------|
|   |                        |                     |                      |                    |

Note: Once top part of form is completed, save and submit form via AskIT Remedy Records Transfer/Disposition service.

Section 2: Historian/Archivist Approvals (DCRM use only)

Part 1: Historical Archive Review

☐ Not Historical ☐ Historical Historical Review Performed By

Date Transferred to Archives

Listed Under TIR(s)

Section 3: Records Center Approval to Proceed with Destruction

Date Approved by

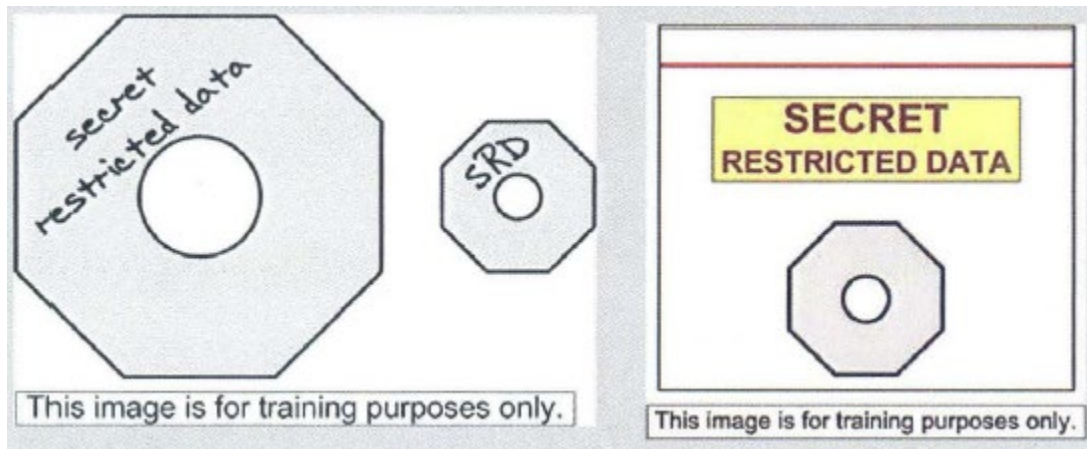
Certificate of Records Destruction Form (8/19) Page 1 of 1

PRINT SAVE CLEAR FORM

For Record Destructions, the Classified Matter Custodian, Document Owner and/or the Records Management Point of Contact (RM-POC) must fill out Form 1704 via the [AskIT request](#) link in the LANL [Records Management Destruction](#) website.

Individual organizations may destroy non-accountable classified documents as long as they have approved classified destruction equipment. Before any records are destroyed, the Records Management Document Control (DCRM) Records Management Program staff must approve the destruction to ensure that the document is not an original, of historical value or on a moratorium hold. This is done by filling out Form 1704.

## Destroying Classified Parts



To destroy classified parts, workers must contact the Office of Classification Group at 667- 0686 for approval of the destruction method. Workers must also document the destruction. The documentation must include the names of the workers who destroyed and witnessed the destruction. The workers destroying and witnessing the destruction must have appropriate clearance, need-to-know and applicable authorizations. Work with your Classified Matter Custodian (CMC) for parts to obtain further guidance regarding classified parts.

## Destroying Accountable Matter



Destruction of accountable matter is not permissible in your work area. Only the accountable library CMC may destroy accountable matter. If you no longer have the need for accountable matter, contact your accountable matter CMC for guidance.

## **Objective 9: Identify Accountability, Emergency Situations and Incident Reporting Requirements**

- Identify the types of accountable classified matter
- Review the general requirements for accountable classified matter
- Identify the accountable libraries
- Procedures for emergency situations
- Uncleared emergency responders
- Actions for handling of classified matter in case of emergency
- Reporting incidents of security concern

In this section we will discuss accountable classified matter. We will identify the different types of accountable classified matter and review the general requirements for accountable classified matter. We will identify the four different accountable libraries that now store all the accountable matter at LANL. We will examine how to handle classified matter during emergency situations and identify requirements for reporting incidents of security concern.

### **Types of Accountable Classified Matter**

Classified matter (electronic, paper, media, or parts) that fall under these categories is considered accountable and must be entered into an accountability system by the accountable library Classified Matter Custodian:

- Top Secret
- Secret Restricted Data (SRD) stored outside a limited area or higher
- Any matter designated as accountable by national, international, or program requirements, for example
  - Sigma 14
  - North Atlantic Treaty Organization (NATO) "Atomal"

### **General Requirements for Accountable Classified Matter**

- Users of accountable matter must handle it appropriately.
- New accountable matter must be marked, assigned a barcode and entered into an accountability system.
- Some working papers may also be accountable.



- Direct any questions about accountable matter to the accountable library CMC or refer to the CMPC Handbook.

The user of any accountable classified matter must ensure that the matter is created, marked, handled, protected, stored, destroyed and accounted for according to the requirements in the CMPC Handbook. When accountable classified matter is created, the creator must ensure the matter is marked as required, assigned a barcode or unique identifier and entered into an accountability system by the accountable library CMC. If a classified working paper or draft may contain accountable classified information, it must be entered into the accountability system pending review. If you have any questions regarding accountable classified matter, contact an accountable library CMC or refer to the CMPC Handbook.

## **Accountable Libraries**

All accountable classified matter has been centralized into accountable libraries.

- All Sigma 14 is stored in the Use Control Site Coordinator (UCSC) accountable library
- Top Secret can be stored in three of the libraries:
  - Weapons Research Services - Secure Information Services (WRS-SIS),
  - The UCSC accountable library, or
  - The Nonproliferation International Security Center (NISC)/Sensitive Compartmented Information Facility (SCIF).

All other accountable matter is stored in the WR-SIS.

## **Procedures for Emergency Situations**

- The RLM must ensure procedures are in place
- Procedures must identify:
  - Notification channels
  - Alternative storage and protection methods
- Safety of workers takes precedence when there is potential for serious injury or death
- Secure classified, if possible

The RLM must ensure that his or her organization has developed procedures for the protection and control of classified matter in emergency situations. The procedures must identify notification channels and alternative storage and protection methods. In an emergency with the potential for serious injury or death, the health and safety of workers take precedence over the need to secure classified matter. If it is possible to do so without compromising worker safety, workers must secure classified matter in a storage container and, if available, activate the intrusion detection system.

## **Uncleared Emergency Responders**

In a life-threatening emergency, classified matter or information may be granted to uncleared emergency responders.

- In a life-threatening emergency, classified matter or information may be granted to uncleared emergency responders.
  - Limit the amount of classified information discussed
  - Limit disclosure to the absolute minimum number of individuals
  - Notify the individual of what specific information is classified and the protection requirements
  - Brief the recipient about not disclosing the information further
- Minimize access by uncleared emergency responders to only those areas affected by the emergency situation.
- Report disclosure of classified information to the Security Incident Team (SIT) Deployed Security Officer (DSO), or a Security Program Lead (SPL).

Special Handling in Case of Emergency:

| Action   |
|--|
| Secure classified matter in a storage container and, if available, activate the intrusion detection system, if emergency is life threatening.                                  |
| If emergency is life threatening, you may leave classified matter unsecured.   |
| Report to your RLM any classified matter or repositories that were left unsecured.   |
| When the area is reoccupied following an emergency, storage containers, vaults and VTR must be inspected to determine if classified matter is missing or has been compromised. |
| Account for all unsecured classified matter following the emergency.   |

*This table outlines actions that can be taken in handling classified matter in the event of an emergency that requires you to leave the work area.*

# Reporting Incidents of Security Concern

**Immediately** notify:

- Security Incident Team (SIT) (phone 665-3505) DSO or a SPL
- Your Responsible Line Manager (RLM)
- Report disclosure of classified information to the Security Incident Team (SIT) Deployed Security Officer (DSO), or a Security Program Lead (SPL).

Do not discuss specific details over an unsecure phone line. Only report that an incident may have occurred and the SIT Inquiry Official will make arrangements to gather the necessary information.

All potential or known violations of DOE, NNSA or LANL security directives and policies must be reported to the Security Incident Team (SIT), Deployed Security Officer (DSO) or a Security Program Lead (SPL). Workers must immediately report any potential or known security incidents to the Security Incident Team and their RLM. If the worker reports to the RLM, the RLM must ensure that the SIT is notified of the discovery of potential or known violations of security directives or policies.

## Classified Matter Contacts

| Topic                    | Contact   |
|--------------------------|---|
| Security Contacts        | <ul style="list-style-type: none"><li>• Deployed Security Officer (DSO)</li><li>• Security Program Leader (SPL)</li></ul>   |
| Classified Matter Issues | <ul style="list-style-type: none"><li>• Classified Matter Custodian (CMC)</li><li>• Derivative Classifier (DC)</li><li>• Responsible Line Manager (RLM) - usually your Group Leader</li><li>• CMPC Team- 665-1802</li><li>• <a href="mailto:cmppc@lanl.gov">cmppc@lanl.gov</a></li><li>• Records Management for destruction of original or historical documents</li></ul> |

It is always better to ask for advice about classified matter protection and control rather than presume what the procedures are. If you have questions, contact these Laboratory resources for assistance.

# Objective 10: Be aware of Points of Contact and Reference documents

- [Classified Matter Protection and Control Handbook, P204-2](#)
- [DOE Order 471.6 Admin Chg.2, "Information Security"](#)
- [Management of Classified Parts Policy, P821-2](#)

Classified Matter Protection and Control is a broad subject. If you feel you need more guidance, the Classified Matter Protection and Control Handbook and DOE order 471.6 Admin Chg.2, Information Security, are good references that will provide more in-depth information. There is also policy specifically for managing classified parts.

---

**You have come to the end of this course. After exiting, you will be required to pass a quiz to receive training credit. The quiz can be accessed separately from the course content list in UTrain.**